

ON PUTATIVE q -ANALOGUES OF THE FANO PLANE AND RELATED COMBINATORIAL STRUCTURES

THOMAS HONOLD AND MICHAEL KIERMAIER

Herrn Professor Armin Leutbecher zum 80. Geburtstag

ABSTRACT. A set \mathcal{F}_q of 3-dimensional subspaces of \mathbb{F}_q^7 , the 7-dimensional vector space over the finite field \mathbb{F}_q , is said to form a q -analogue of the Fano plane if every 2-dimensional subspace of \mathbb{F}_q^7 is contained in precisely one member of \mathcal{F}_q . The existence problem for such q -analogues remains unsolved for every single value of q . Here we report on an attempt to construct such q -analogues using ideas from the theory of subspace codes, which were introduced a few years ago by Koetter and Kschischang in their seminal work on error-correction for network coding. Our attempt eventually fails, but it produces the largest subspace codes known so far with the same parameters as a putative q -analogue. In particular we find a ternary subspace code of new record size 6977, and we are able to construct a binary subspace code of the largest currently known size 329 in an entirely computer-free manner.

1. INTRODUCTION

The Fano plane $\mathcal{F} = \text{PG}(2, \mathbb{F}_2) = \text{PG}(\mathbb{F}_2^3/\mathbb{F}_2)$, the coordinate geometry derived from a 3-dimensional vector space over the binary field \mathbb{F}_2 , is the smallest nontrivial model of an abstract projective geometry. It has 7 points and 7 lines, represented by the one- and two-dimensional subspaces of $\mathbb{F}_2^3/\mathbb{F}_2$, respectively; each line contains 3 points and each point is on 3 lines; any two distinct points are contained in a unique line and any two distinct lines intersect in a unique point. Myriads of other finite models of a projective geometry exist—for each integer $n \geq 2$ and prime power $q > 1$ the n -dimensional coordinate geometry $\text{PG}(n, \mathbb{F}_q) = \text{PG}(\mathbb{F}_q^{n+1}/\mathbb{F}_q)$ over the finite field \mathbb{F}_q , and in the planar case many additional examples with the same parameters as some $\text{PG}(2, \mathbb{F}_q)$.

The Fano plane $\mathcal{F} = \text{S}(2, 3, 7)$ is also the smallest nontrivial example of a *Steiner system* $\text{S}(t, k, v)$, which refers to a v -set V (*point set*) and a set of k -subsets of V (*blocks*) having the property that any t -subset of V is contained in exactly one block. The more general concept of a combinatorial t -(v, k, λ) design relaxes the requirement “exactly one block” to a “constant number λ of blocks”. Many constructions of

t -(v, k, λ) designs are known (including the construction of nontrivial t -designs for all positive integers t by Teirlinck [30]), but comparatively few Steiner systems and still no one at all with $t > 5$).¹

This article is concerned with vector space analogues of \mathcal{F} in the following sense:

Definition 1. *Let $q > 1$ be a prime power. A set \mathcal{F}_q of 3-dimensional subspaces of $\mathbb{F}_q^7/\mathbb{F}_q$ (or any other 7-dimensional vector space V over \mathbb{F}_q) is said to be a q -analogue of the Fano plane if every 2-dimensional subspace of \mathbb{F}_q^7 (respectively, V) is contained in a unique member of \mathcal{F}_q .*

In projective geometry language, a q -analogue of the Fano plane is a set \mathcal{F}_q of planes in $\text{PG}(6, \mathbb{F}_q)$ such that any pair of distinct points (equivalently, any line) is contained in exactly one plane $E \in \mathcal{F}_q$. In other words, the planes in \mathcal{F}_q , when identified with sets of lines, should form an exact cover (i.e., a partition) of the line set of $\text{PG}(6, \mathbb{F}_q)$.

Before going any further, we should remark that at the time of writing this article virtually nothing is known about the existence of such structures—neither existence nor non-existence of a q -analogue of the Fano plane has been proved for a single instance of q . Even in the smallest case $q = 2$, where a putative 2-analogue \mathcal{F}_2 would have to contain 381 of the 11811 planes of $\text{PG}(6, \mathbb{F}_2)$, a computer search seems infeasible at present.

P. Cameron [6] introduced the concept of a *design over a finite field* as a vector space analogue (“ q -analogue”, if the underlying field is \mathbb{F}_q) of combinatorial designs: A t -(v, k, λ) design over \mathbb{F}_q is a set \mathcal{C} of k -dimensional subspaces of $\mathbb{F}_q^v/\mathbb{F}_q$ (or any other v -dimensional vector space V over \mathbb{F}_q) with the property that every t -dimensional subspace of \mathbb{F}_q^v (respectively, V) is contained in exactly λ members of \mathcal{C} . The first nontrivial examples of such designs were constructed by S. Thomas [31]. These “Thomas designs” have $q = 2$ and form an infinite family with parameters 2-($v, 3, 7$), where $v \equiv \pm 1 \pmod{6}$ and $v \geq 7$. Taking the ambient space as the finite field \mathbb{F}_{2^v} , one may construct the 2-($v, 3, 7$) Thomas design \mathcal{T}_v as the set of all 3-dimensional \mathbb{F}_2 -subspaces $\langle x, y, z \rangle \subset \mathbb{F}_{2^v}$ spanned by the $2^v - 2$ non-rational points in $\text{PG}(2, \mathbb{F}_{2^v})$ of a rational conic (relative to \mathbb{F}_2). For example, we can take all points $(x : y : z) \neq (1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$ on the conic $xy + yz + zx = 0$, resulting in $\mathcal{T}_v = \left\{ \langle x, y, \frac{xy}{x+y} \rangle; x, y \in \mathbb{F}_{2^v}^\times \text{ distinct} \right\}$.² Although several further constructions of designs over finite fields are now known (including the existence of nontrivial t -designs over \mathbb{F}_q for arbitrarily large t in [14]), the subject has turned out considerably more difficult

¹We should note here that recently Keevash [22] has given a non-constructive proof of the existence of Steiner systems for all values of t .

²Checking the design property is somewhat tedious, but at least we can see immediately from the definition that \mathcal{T}_v has the required $(2^v - 2)/6 \times (2^v - 1) = (2^v - 1)(2^{v-1} - 1)/3$ blocks.

than ordinary combinatorial design theory. For example, no nontrivial 4-design over a finite field is known at present.

At the end of [31] Thomas briefly discussed q -analogues $S_q(t, k, v)$ of Steiner systems (i.e. t -($v, k, 1$) designs over \mathbb{F}_q) and in particular the smallest feasible parameter case $S_2(2, 3, 7)$. Such a 2-analogue of the Fano plane would consist of $381 = 3 \times 127$ three-dimensional subspaces of \mathbb{F}_2^7 (cf. Lemma 2), and it was conceivable to construct it as the union of 3 orbits of a Singer subgroup of $\text{GL}(2, 7)$. However, as Thomas reported, this construction is impossible.

A few years ago interest in designs over finite fields was revived through the observation by R. Koetter and F. Kschischang [25] that sets of subspaces of a vector space over a finite field (*subspace codes*) can be used as “distributed channel codes” for error-resilient transmission of information in packet networks. Considering q (*symbol alphabet of the packet network*) and the ambient vector space dimension v (*packet length*) as fixed and restricting attention to *constant-dimension* codes (i.e the dimension k of all codewords is the same), the best performance is achieved by using subspace codes \mathcal{C} that have simultaneously large size $\#\mathcal{C} = |\mathcal{C}|$ and small maximum dimension of an intersection between distinct codewords. Denoting this dimension by $t - 1$, we have that t is the smallest positive integer such that every t -dimensional subspace of \mathbb{F}_q^v is contained in at most one codeword of \mathcal{C} . Subspace codes thus satisfy a weaker form of the defining condition for Steiner systems over finite fields.³ A standard double-counting argument gives $\#\mathcal{C} \times \begin{bmatrix} k \\ t \end{bmatrix}_q \leq \begin{bmatrix} v \\ t \end{bmatrix}_q$ with equality if and only if each t -dimensional subspace of \mathbb{F}_q^v is contained in precisely one codeword of \mathcal{C} . Hence Steiner systems over finite fields are optimal as subspace codes.⁴

In the sequel we will exclusively be concerned with subspace codes of constant dimension $k = 3$, so-called *plane subspace codes*, and packet length $v = 7$. Plane subspace codes with $t = 3$ are trivial—the whole plane set of $\text{PG}(6, \mathbb{F}_q)$ forms such a code. Plane subspace codes with $t = 1$ consist of pairwise skew planes and are known as *partial plane spreads* in Finite Geometry. The maximum size of a partial plane spread in $\text{PG}(6, \mathbb{F}_q)$ is known to be $q^4 + 1$ from the work of Beutelspacher

³The difference is quite similar to that between *linear spaces* (two distinct points are connected by exactly one line) and *partial linear spaces* (two distinct points are connected by at most one line), as defined in Incidence Geometry. Subspace codes could thus be called “partial Steiner systems over finite fields”.

⁴From this we also see that the parameters q, t, k, v of an $S_q(t, k, v)$, like those of an ordinary Steiner system, must obey certain *integrality conditions*. In fact the existence of an $S_q(t, k, v)$ implies the existence of an $S_q(t - 1, k - 1, v - 1)$. The so-called *derived designs*, which are formed by the blocks through a fixed 1-dimensional subspace of \mathbb{F}_q^v , have these parameters. Hence a necessary condition for the existence of an $S_q(t, k, v)$ is that $\begin{bmatrix} v-s \\ t-s \end{bmatrix}_q / \begin{bmatrix} k-s \\ t-s \end{bmatrix}_q$ must be an integer for $1 \leq s \leq t$.

[2, Th. 4.1].⁵ This leaves the case $t = 2$ considered so far as the only unresolved case. Restricting attention to this case, we will from now on tacitly assume that “subspace code” includes the assumption $t = 2$.

More than 25 years have passed since Thomas’ fundamental work [31] and the existence problem for q -analogues of the Fano plane is still undecided. On the other hand, serious attempts, often relying on quite sophisticated computational methods, have been made to construct large subspace codes—including the parameter set of a putative 2-analogue. These will now be briefly reviewed. Accordingly, let \mathcal{C} be a binary plane subspace code with $v = 7$ or, in geometric terms, a set of planes in $\text{PG}(6, \mathbb{F}_2)$ mutually intersecting in at most a point. As discussed above, we have $\#\mathcal{C} \leq 381$ with equality if and only if \mathcal{C} is a 2-analogue of the Fano plane. The first nontrivial lower bound on the maximum size of \mathcal{C} was established by Koetter and Kschischang [25], who showed that $\#\mathcal{C} = 256$ is realized by a so-called lifted maximum-rank distance code (LMRD code). Kohnert and Kurz [26] improved this to $\#\mathcal{C} = 304$, employing a computer search for plane subspace codes in $\text{PG}(6, \mathbb{F}_2)$ with an automorphism of order 21 acting irreducibly on a hyperplane. The current record is $\#\mathcal{C} = 329$ and was established by Braun and Reichelt in [5] using a refinement of this method. In [21], as part of the classification of all optimal plane subspace codes in the smaller geometry $\text{PG}(5, \mathbb{F}_2)$, an optimal $\#\mathcal{C} = 77$ subspace code was constructed by first expurgating an LMRD code (size 64) to a particular subspace code of size 56 and then augmenting this code by 21 further planes. As shown in [27], the underlying idea can be used to provide an alternative construction of a plane subspace code of size 329 in $\text{PG}(6, \mathbb{F}_2)$.

In this paper we will develop a general framework for constructing large plane subspace codes in $\text{PG}(6, \mathbb{F}_q)$ along the lines of [21, 27], but also introducing several new ideas (in Sections 4 and 5). Our main results are the construction of a general q -ary subspace code \mathcal{C} of size $q^8 + q^5 + q^4 - q - 1$, whose planes meet a fixed solid (3-flat) of $\text{PG}(6, \mathbb{F}_q)$ in at most a point (Theorem 3 in Section 5), and a detailed analysis of the extension problem for \mathcal{C} (or rather, a distinguished subcode $\mathcal{C}_0 \subset \mathcal{C}$) by planes meeting S in a line, which enables us to give the first computer-free construction of a plane subspace code of size 329 in $\text{PG}(6, \mathbb{F}_2)$ (see above) and a computer-aided construction of a plane subspace code of size 6977 in $\text{PG}(6, \mathbb{F}_3)$ (Section 6, in particular Theorem 4). Theorem 3 improves the best previously known construction for general q [32], and the ternary subspace code of size 6977 is by way the largest known code with its parameters. In order to make the paper self-contained, we provide a general introduction to the combinatorics of subspace

⁵In general, the maximum size of a partial plane spread in $\text{PG}(v-1, \mathbb{F}_q)$ is known for $v \equiv 0, 1 \pmod 3$ (all q) and for $q = 2$ (all v); for the latter see [12].

codes in Section 2 and an account of related previous subspace code constructions in Section 3.

In the sequel \mathcal{F}_q always denotes a putative q -analogue of the Fano plane. The term “dimension” refers to vector space dimension, but otherwise geometric language will be extensively used. When referring to the geometric dimension of a t -dimensional subspace of $\mathbb{F}_q^v/\mathbb{F}_q$, we use the term “ $(t-1)$ -flat of $\text{PG}(v-1, \mathbb{F}_q)$ ”.

Let us close this introduction with a remark on vector space analogues of the Fano plane over infinite fields. Using transfinite recursion, it is fairly easy to show that for any field K with $|K| = \infty$ a K -analogue \mathcal{F}_K , defined as in Def. 1, does exist. For example, in the case $K = \mathbb{Q}$ we can enumerate the lines of $\text{PG}(6, \mathbb{Q})$ as L_0, L_1, L_2, \dots and recursively define sets $\mathcal{E}_0 = \emptyset, \mathcal{E}_1, \mathcal{E}_2, \dots$ of planes as follows: If \mathcal{E}_n already contains a plane $E \supset L_n$, we set $\mathcal{E}_{n+1} = \mathcal{E}_n$; otherwise, among the planes containing L_n there exists a plane E that has no line in common with any of the planes in \mathcal{E}_n , and we set $\mathcal{E}_{n+1} = \mathcal{E}_n \cup \{E\}$.⁶ It is then readily verified that $\mathcal{F}_{\mathbb{Q}} = \bigcup_{n=0}^{\infty} \mathcal{E}_n$ is the required \mathbb{Q} -analogue of \mathcal{F} .

In fact it is even true that the plane set of any geometry $\text{PG}(v-1, K)$, $|K| = \infty$, $v \geq 5$, can be partitioned into Steiner systems $S_K(2, 3, v)$; see [7] for details.

2. COUNTING PRELIMINARIES

Let us first recall that the number of k -dimensional subspaces of an n -dimensional vector space over \mathbb{F}_q is given by the Gaussian binomial coefficient

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)},$$

which is polynomial in q of degree $k(n-k)$ and satisfies $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q = q^{k(n-k)} \cdot \begin{bmatrix} n \\ k \end{bmatrix}_{q^{-1}}$. In particular the number of points (and hyperplanes) of $\text{PG}(n-1, \mathbb{F}_q)$ is equal to

$$\begin{bmatrix} n \\ 1 \end{bmatrix}_q = \begin{bmatrix} n \\ n-1 \end{bmatrix}_q = \frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1}.$$

Subspaces U of $\mathbb{F}_q^n/\mathbb{F}_q$ of dimension k are in one-to-one correspondence with matrices $\mathbf{U} = \text{cm}(U) \in \mathbb{F}_q^{k \times n}$ in reduced row-echelon form via $U = \langle \text{cm}(U) \rangle$, the row space of the matrix $\text{cm}(U)$, and $\mathbf{U} = \text{cm}(\langle \mathbf{U} \rangle)$.⁷

⁶More precisely, the first plane with this property, according to some predefined order E_0, E_1, E_2, \dots on the set of planes of $\text{PG}(6, \mathbb{Q})$, is chosen. The existence of such a plane follows from the fact that L_n and the finitely many solids (3-flats) $E' + L_n$, $E' \in \mathcal{E}_n$ a plane intersecting L_n (necessarily in a point), cannot cover all points of $\text{PG}(6, \mathbb{Q})$.

⁷The name ‘cm’ resembles “canonical matrix”.

If $\text{cm}(U)$ has pivot columns in positions $1 \leq j_1 < j_2 < \cdots < j_k \leq n$ then the number of unspecified entries (“wildcards”) in $\text{cm}(U)$ is $i = 1(j_2 - j_1 - 1) + 2(j_3 - j_2 - 1) + \cdots + (k-1)(j_k - j_{k-1} - 1) + k(n - j_k)$ and determines a partition of the integer i into at most $n - k$ parts of size at most k .⁸ The coefficient a_i of q^i in $\begin{bmatrix} n \\ k \end{bmatrix}_q$ counts the number of such partitions, and consequently the monomial $a_i q^i$ counts the k -dimensional subspaces of \mathbb{F}_q^n having exactly i unspecified entries in their canonical matrix.

These and a few additional observations allow for “almost everything” in $\text{PG}(n-1, \mathbb{F}_q) = \text{PG}(\mathbb{F}_q^n / \mathbb{F}_q)$ to be counted. Consider, for example, any solid (3-flat) S in $\text{PG}(6, \mathbb{F}_q)$ and count the planes of $\text{PG}(6, \mathbb{F}_q)$ according to their intersection size with S . There are q^{12} planes disjoint from S , corresponding to the q^{12} canonical matrices

$$\begin{pmatrix} 1 & 0 & 0 & * & * & * & * \\ 0 & 1 & 0 & * & * & * & * \\ 0 & 0 & 1 & * & * & * & * \end{pmatrix}$$

(for this arrange coordinates such that $S = (0, 0, 0, *, *, *, *)$); there are $q^6 \cdot \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q = q^6(q^2 + q + 1)(q^3 + q^2 + q + 1)$ planes E meeting S in a point (considering the hyperplane $H = E + S$ and the intersection point $P = E \cap S$ as fixed, these correspond to lines disjoint from the plane S/P in $H/P \cong \text{PG}(4, \mathbb{F}_q)$, of which there are q^6 corresponding to the canonical matrix shape $\begin{pmatrix} 1 & 0 & * & * & * & * \\ 0 & 1 & * & * & * & * \\ 0 & 0 & 1 & * & * & * \end{pmatrix}$); there are $q^2 \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^2(q^2 + q + 1)(q^4 + q^3 + 2q^2 + q + 1)$ planes E meeting S in a line (considering the 4-flat $T = E + S$ and the line $L = E \cap S$ as fixed, these correspond to points outside the line S/L in $T/L \cong \text{PG}(2, \mathbb{F}_q)$);⁹ and finally, there are $\begin{bmatrix} 4 \\ 3 \end{bmatrix}_q = \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q = q^3 + q^2 + q + 1$ planes contained in S .

Now let \mathcal{C} be a set of planes in $\text{PG}(6, \mathbb{F}_q)$ mutually intersecting in at most a point (a plane subspace code in the terminology of Section 1). Fixing any solid S in $\text{PG}(6, \mathbb{F}_q)$, we can count how many planes in \mathcal{C} intersect S in a subspace of dimension $i \in \{0, 1, 2, 3\}$. This leads to the concept of “spectra” (or “intersection vectors”) with respect to solids, which already capture a great deal of structural information about \mathcal{C} .

Definition 2. *The spectrum (or intersection vector) of \mathcal{C} with respect to S is defined as the 4-tuple $\alpha(S) = (\alpha_0(S), \alpha_1(S), \alpha_2(S), \alpha_3(S))$, $\alpha_i(S) = \#\{E \in \mathcal{C}; \dim(E \cap S) = i\}$, of non-negative integers.*

⁸The number of (positive) parts is $\sum_{\nu=1}^{k-1} (j_{\nu+1} - j_{\nu} - 1) + n - j_k = n - k - (j_1 - 1)$.

⁹Here we have used $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^4 + q^3 + 2q^2 + q + 1$, which follows from counting the partitions into at most 2 parts of size ≤ 2 according to their sum: $0 = 0$, $1 = 1$, $2 = 2 = 1 + 1$, $3 = 2 + 1$, $4 = 2 + 2$.

The example counting problem discussed above amounts to determining the spectrum of the whole plane set of $\text{PG}(6, \mathbb{F}_q)$ with respect to any solid, which turned out to be a constant independent of S .¹⁰

Lemma 1. *Let \mathcal{C} be a plane subspace code of size M in $\text{PG}(6, \mathbb{F}_q)$ and S any solid in $\text{PG}(6, \mathbb{F}_q)$. The spectrum $\alpha = \alpha(S)$ of \mathcal{C} with respect to S satisfies $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = M$ and the following system of linear inequalities:*

$$\begin{aligned} \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \cdot \alpha_0 + q^2 \alpha_1 &\leq q^8 \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \\ (q+1)\alpha_1 + (q^2+q)\alpha_2 &\leq q^3 \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \cdot \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q \\ \alpha_2 + \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \cdot \alpha_3 &\leq \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q \\ \alpha_3 &\leq 1 \end{aligned}$$

The explicit form of all four inequalities is obtained by inserting $\begin{bmatrix} 3 \\ 1 \end{bmatrix}_q = q^2 + q + 1$, $\begin{bmatrix} 4 \\ 1 \end{bmatrix}_q = q^3 + q^2 + q + 1$ and $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^4 + q^3 + 2q^2 + q + 1 = (q^2 + 1)(q^2 + q + 1)$.

Proof. The equation $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = M$ is clear from the definition of the spectrum. The first three inequalities are proved by counting the line-plane pairs (L, E) with $E \in \mathcal{C}$, $L \subset E$ and $\dim(L \cap S) = i$ for $i = 0, 1, 2$, respectively, in two ways and using the fact that every line is contained in at most one plane of \mathcal{C} (and hence counted at most once on the left-hand side). The right-hand side of the corresponding inequality gives the total number of lines L with $\dim(L \cap S) = i$. Finally, since two distinct planes of \mathcal{C} generate an at least 5-dimensional space, S can contain at most one plane of \mathcal{C} and thus $\alpha_3 \in \{0, 1\}$. \square

Lemma 1 can be used to derive quite restrictive conditions on the parameters of a putative q -analogue of the Fano plane. This is the subject of Lemma 2. For the statement of the lemma recall that the cyclotomic polynomials $\Phi_n(X) \in \mathbb{Z}[X]$, defined recursively by $X^n - 1 = \prod_{d|n} \Phi_d(X)$ for $n \in \mathbb{N}$, satisfy $\Phi_p(X) = X^{p-1} + X^{p-2} + \dots + X + 1$ for prime numbers p , as well as $\Phi_6(X) = X^2 - X + 1$. In terms of cyclotomic polynomials the number of points of $\text{PG}(n-1, \mathbb{F}_q)$ is $\begin{bmatrix} n \\ 1 \end{bmatrix}_q = \frac{q^n - 1}{q - 1} = \prod_{d|n, d \neq 1} \Phi_d(q)$.

Lemma 2. *If a q -analogue \mathcal{F}_q of the Fano plane exists, it must have the following properties:*

(i) *The number of planes in \mathcal{F}_q is*

$$\begin{aligned} \#\mathcal{F}_q &= \Phi_7(q)\Phi_6(q) = (q^6 + q^5 + q^4 + q^3 + q^2 + q + 1)(q^2 - q + 1) \\ &= q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1, \end{aligned}$$

¹⁰The latter also follows from the observation that $\text{GL}(7, \mathbb{F}_q)$ acts transitively on the set of all plane-solid pairs (E, S) with fixed intersection dimension i .

with $\Phi_6(q)\Phi_3(q) = q^4 + q^2 + 1$ planes passing through each point of $\text{PG}(6, \mathbb{F}_q)$.

(ii) The spectrum of \mathcal{F}_q with respect to solids takes the two values

$$\alpha_0 = (q^8 - q^7 + q^3, q^7 + q^6 + q^5 - q^3 - q^2 - q, q^4 + q^3 + 2q^2 + q + 1, 0),$$

$$\alpha_1 = (q^8 - q^7, q^7 + q^6 + q^5, q^4 + q^3 + q^2, 1)$$

with corresponding frequencies

$$f_0 = q^{12} + q^{10} + q^9 + q^8 + q^7 + q^6 + q^4,$$

$$f_1 = q^{11} + q^{10} + 2q^9 + 3q^8 + 3q^7 + 4q^6 + 4q^5 + 3q^4 + 3q^3 + 2q^2 + q + 1.$$

Proof. For a q -analogue of the Fano plane the first three inequalities in Lemma 1 are in fact equalities (for any solid S) and, conversely, this property (even if it holds only for one particular solid S) implies that \mathcal{C} must be a q -analogue of the Fano plane.

Further, the triangular shape of the system implies that each of the two possible choices $\alpha_3 \in \{0, 1\}$ leads to a unique solution for $\alpha_1, \alpha_2, \alpha_3$.

In the first case ($\alpha_3 = 0$) we obtain

$$\alpha_2 = q^4 + q^3 + 2q^2 + q + 1 = \Phi_4(q)\Phi_3(q),$$

$$\begin{aligned} \alpha_1 &= \frac{1}{q+1} \left(q^3 \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q - q(q+1)\alpha_2 \right) \\ &= \frac{1}{q+1} (q^3 \cdot \Phi_3(q) \cdot \Phi_4(q)\Phi_2(q) - q \cdot \Phi_2(q) \cdot \Phi_4(q)\Phi_3(q)) \\ &= (q^3 - q)\Phi_4(q)\Phi_3(q) = q \cdot \Phi_4(q)\Phi_3(q)\Phi_2(q)\Phi_1(q) \\ &= q(q^4 - 1)(q^2 + q + 1) = q^7 + q^6 + q^5 - q^3 - q^2 - q, \\ \alpha_0 &= q^8 - \frac{q^2}{q^2 + q + 1} \cdot \alpha_1 = q^8 - q^7 + q^3, \end{aligned}$$

as asserted. The second case ($\alpha_3 = 1$) is done similarly.

Finally, a solid S of $\text{PG}(6, \mathbb{F}_q)$ has $\alpha_3(S) = 1$ iff it contains a plane of \mathcal{F}_q . The number of such solids is

$$\begin{aligned} f_1 &= \#\mathcal{F}_q \cdot \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q = \Phi_7(q)\Phi_6(q)\Phi_4(q)\Phi_2(q) \\ &= q^{11} + q^{10} + 2q^9 + 3q^8 + 3q^7 + 4q^6 + 4q^5 + 3q^4 + 3q^3 + 2q^2 + q + 1, \end{aligned}$$

and the number of solids with $\alpha_3(S) = 0$ is

$$\begin{aligned} f_0 &= \begin{bmatrix} 7 \\ 4 \end{bmatrix}_q - f_1 = \begin{bmatrix} 7 \\ 3 \end{bmatrix}_q - f_1 \\ &= \Phi_7(q)\Phi_6(q)\Phi_5(q) - \Phi_7(q)\Phi_6(q)\Phi_4(q)\Phi_2(q) \\ &= \#\mathcal{F}_q \cdot q^4 = q^{12} + q^{10} + q^9 + q^8 + q^7 + q^6 + q^4, \end{aligned}$$

completing the proof. \square

Remark 1. *More general results on the intersection structure of a putative q -analogue of the Fano plane can be found in [24, Sect. 4].*

Performing the same computations, mutatis mutandis, for putative Steiner systems $S_q(2, 3, v)$ with arbitrary ambient space dimension v yields non-integral solutions and hence excludes the existence of an $S_q(2, 3, v)$ for $v \equiv 0, 2, 4, 5 \pmod{6}$. Thus an $S_q(2, 3, v)$ can exist only for $v \in \{7, 9, 13, 15, 19, 21, 25, 27, \dots\}$. For the particular case $q = 2$, $v = 13$ existence has been proved in [4], providing the only known nontrivial example of a Steiner system over a finite field. This remarkable result was the outcome of a computer search for Steiner systems $S_2(2, 3, 13)$ invariant under the normalizer of a Singer subgroup of $GL(13, \mathbb{F}_2)$, a group of order $(2^{13} - 1) \cdot 13 = 106483$, and of course facilitated by the fact that Steiner systems $S_2(2, 3, 13)$ with this additional structure exist.¹¹

3. AUGMENTED LMRD CODES

The initial subspace code constructions by Koetter, Kschischang and Silva [25, 29] were based on the observation that the dimension of the intersection of two k -dimensional subspaces U, V of $\mathbb{F}_q^v/\mathbb{F}_q$ with canonical matrices of the special form $(\mathbf{I}_k|\mathbf{A})$, $(\mathbf{I}_k|\mathbf{B})$ can be expressed through the rank of the matrix $\mathbf{A} - \mathbf{B} \in \mathbb{F}_q^{k \times (v-k)}$. In fact it is easily seen that $U \cap V = \{(\mathbf{x}|\mathbf{x}\mathbf{A}); \mathbf{x} \in \text{Ker}(\mathbf{A} - \mathbf{B})\} \cong \text{Ker}(\mathbf{A} - \mathbf{B})$ (the left kernel of $\mathbf{A} - \mathbf{B}$) and thus $\dim(U \cap V) = k - \text{rk}(\mathbf{A} - \mathbf{B})$.

From earlier work of Delsarte [8] (and independently Gabidulin and Roth [18, 28]) the maximum number of matrices in $\mathbb{F}_q^{m \times n}$ having pairwise rank distance at least d is known to be $q^{(m-d+1)n}$, provided that $m \leq n$.¹² Subsets $\mathcal{A} \subseteq \mathbb{F}_q^{m \times n}$ of size $q^{(m-d+1)n}$ with $\text{rk}(\mathbf{A} - \mathbf{B}) \geq d$ for all pairs of distinct $\mathbf{A}, \mathbf{B} \in \mathcal{A}$ are known as $(m, n, m - d + 1)$ *maximum rank distance (MRD) codes*. Via the *lifting construction* $\mathcal{A} \rightarrow \mathcal{L} \subseteq \mathbb{F}_q^{m \times (m+n)}$, $\mathbf{A} \mapsto \langle (\mathbf{I}_m|\mathbf{A}) \rangle$ they give rise to subspace codes \mathcal{L} in $\text{PG}(m+n-1, \mathbb{F}_q)$ of size $\#\mathcal{L} = \#\mathcal{A} = q^{(m-d+1)n}$, constant dimension m and maximum intersection dimension $m - d$, as we have indicated above. These subspace codes are called *lifted maximum rank distance (LMRD) codes*.

In the case of interest to us we can find q^8 matrices in $\mathbb{F}_q^{3 \times 4}$ at pairwise rank distance ≥ 2 and lift these to a plane LMRD code in $\text{PG}(6, \mathbb{F}_q)$ of size q^8 with maximum intersection dimension 1. This gives the lower bound $\#\mathcal{C} \geq q^8$ for the maximum size of a plane subspace code in

¹¹An $S_2(2, 3, 13)$ contains as many as $\frac{(2^{13}-1)(2^{12}-1)}{21} = 1597245$ planes out of a total of $\begin{bmatrix} 13 \\ 3 \end{bmatrix}_2 = 3269560515$ planes in $\text{PG}(12, \mathbb{F}_2)$, rendering any unrestricted search for such a structure completely infeasible.

¹²The assumption $m \leq n$ imposes no essential restriction, since matrices can be transposed without changing the rank.

$\text{PG}(6, \mathbb{F}_q)$, which is already of the same asymptotic order as a putative 2-analogue of the Fano plane ($\#\mathcal{F}_q = q^8 + q^6 + q^5 + q^4 + q^3 + q^2 + 1$).

Following the work in [25, 29], several constructions have been proposed for augmenting LMRD codes without increasing t . (Note that increasing t sacrifices the error-correction capabilities of the original subspace code.) All these constructions are variants of the so-called *echelon-Ferrers* construction introduced in [13], which combines subspace codes in different Schubert cells of the corresponding Grassmannian in a certain way.¹³ We will not delve into this further, but instead only mention that the maximum size of an augmented LMRD code obtained in this way is $\#\mathcal{C} = q^8 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^8 + q^4 + q^3 + 2q^2 + q + 1$ and provide a different construction of such a code below.

In fact the bound $\#\mathcal{C} \leq q^8 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$ holds for any plane subspace code in $\text{PG}(6, \mathbb{F}_q)$ containing an LMRD code. This is a consequence of the following lemma, which could be easily generalized to arbitrary packet length v .

Lemma 3. *Let \mathcal{L} be a plane LMRD code in $\text{PG}(6, \mathbb{F}_q)$ and $S = (0, 0, 0, *, *, *, *)$ the special solid defined by $x_1 = x_2 = x_3 = 0$. Then the planes in \mathcal{L} cover all lines that are disjoint from S (and no other lines).*

Proof. A line L disjoint from S has a canonical matrix of the form $(\mathbf{Z}|\mathbf{B})$ with $\mathbf{Z} \in \mathbb{F}_q^{2 \times 3}$ in canonical form and $\mathbf{B} \in \mathbb{F}_q^{2 \times 4}$ arbitrary. Now let \mathcal{A} be the matrix code corresponding to \mathcal{L} and consider the map $\mathcal{A} \rightarrow \mathbb{F}_q^{2 \times 4}$, $\mathbf{A} \mapsto \mathbf{Z}\mathbf{A}$. Since $\text{rk}(\mathbf{Z}) = 2$ and the minimum nonzero rank in \mathcal{A} is 2, this map must be injective, hence also surjective. Thus there exists $\mathbf{A} \in \mathcal{A}$ such that $\mathbf{B} = \mathbf{Z}\mathbf{A}$, implying $\text{cm}(L) = \mathbf{Z}(\mathbf{I}_3|\mathbf{A})$. The latter just says that L is contained in the plane $\langle (\mathbf{I}_3|\mathbf{A}) \rangle \in \mathcal{L}$. \square

With the aid of this lemma the bound $\#\mathcal{C} \leq q^8 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$ is established as follows: A fortiori \mathcal{C} covers every line disjoint from S and hence cannot contain a plane meeting S in a point (as such a plane would contain lines disjoint from S). Thus, apart from the planes in \mathcal{L} , it contains only planes meeting S in a line or planes entirely contained in S . The number of such planes is bounded by the total number of lines in S , yielding the bound. (Moreover, the bound can be achieved only if no plane of \mathcal{C} is contained in S .)

We close this section with an alternative construction of an augmented plane LMRD code in $\text{PG}(6, \mathbb{F}_q)$ of size $q^8 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$. Such a code was first constructed in [32]. Our construction uses the existence of a *line packing* of $\text{PG}(3, \mathbb{F}_q)$, which refers to a partition of the line set into line spreads, where a *line spread* is itself defined as a partition

¹³“Schubert cell” refers to the set of all subspaces whose canonical matrices have their pivot columns fixed.

of the point set into lines (the same as a partial line spread that covers all points).¹⁴ Line packings of $\text{PG}(3, \mathbb{F}_q)$ exist for all prime powers $q > 1$; cf. [1, 10]. Since line spreads of $\text{PG}(3, \mathbb{F}_q)$ have size $q^2 + 1$ and $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = (q^2 + 1)(q^2 + q + 1)$, the number of line spreads in a line packing is $q^2 + q + 1$.

Theorem 1. *Any plane LMRD code \mathcal{L} in $\text{PG}(6, \mathbb{F}_q)$ can be augmented by $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^4 + q^3 + 2q^2 + q + 1$ further planes to yield a plane subspace code \mathcal{C} of size $\#\mathcal{C} = q^8 + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^8 + q^4 + q^3 + 2q^2 + q + 1$.¹⁵*

Proof. Choose a packing $\mathcal{P} = \{\mathcal{P}_1, \dots, \mathcal{P}_{q^2+q+1}\}$ of $\text{PG}(S/\mathbb{F}_q) \cong \text{PG}(3, \mathbb{F}_q)$, and let $\{P_1, \dots, P_{q^2+q+1}\}$ be a set of points in $\text{PG}(6, \mathbb{F}_q)$ forming a set of representatives for the $q^2 + q + 1$ 4-flats containing S .¹⁶ For $1 \leq i \leq q^2 + q + 1$ connect the point P_i to all $q^2 + 1$ lines L_{ij} in \mathcal{P}_i to form a set of $(q^2 + 1)(q^2 + q + 1)$ planes $E_{ij} = P_i + L_{ij}$. We claim that $\mathcal{C} = \mathcal{L} \cup \{E_{ij}\}$ has the required property.

Clearly the “new” planes E_{ij} cover no line disjoint from S and each line in S exactly once. Now suppose, for contradiction, that L is a line meeting S in a point P and contained in two different new planes $E = P_i + L_{ij}$, $E' = P_{i'} + L_{i'j'}$. Then L must meet both L_{ij} and $L_{i'j'}$ in P , whence L_{ij} and $L_{i'j'}$ intersect and $i \neq i'$. But the 4-flats $F_i = L + S = F_{i'}$ coincide, contradiction! \square

The subspace code \mathcal{C} of Theorem 1 is quite small in comparison with the codes constructed later in our main theorems. But we feel that the construction method is of independent interest and have included it for this reason.

4. FIRST EXPURGATING AND THEN AUGMENTING

In this section we describe the basic idea used in [21] to overcome the size restriction imposed on subspace codes containing LMRD codes, tailored (and generalized) to the case of plane subspace codes in $\text{PG}(6, \mathbb{F}_q)$ with arbitrary q .

Given a plane LMRD code \mathcal{L} in $\text{PG}(6, \mathbb{F}_q)$, we must obviously remove some of the q^8 planes in \mathcal{L} first and then augment the resulting subcode $\mathcal{L}_0 \subset \mathcal{L}$ as far as possible. What is the best way to do this? The “removed” set of planes \mathcal{L}_1 , of size $\#\mathcal{L}_1 = M_1$ say, covers $(q^2 + q + 1)M_1$ lines disjoint from the special solid $S = (0, 0, 0, 0, *, *, *)$, which become *free lines* of \mathcal{L}_0 in the sense that any *new plane* added to \mathcal{L}_0 , which

¹⁴Line packings form a projective analogue of the standard resolution of the line set of an affine plane into parallel classes.

¹⁵We remind the reader one last time that all subspace codes considered (including LMRD codes) have $t = 2$ (maximum intersection dimension 1).

¹⁶By this we mean $P_i \notin S$ and the 4-flats $F_i = P_i + S$, $1 \leq i \leq q^2 + q + 1$, account for all 4-flats above S .

contains only lines disjoint from S that are free, will not increase t (i.e., introduce a multiple line cover). Of course we are only interested in adding new planes which meet S in a point at this stage, since this is the only way to go beyond the construction in Section 3. In this case, provided an exact rearrangement of the free lines into new planes is possible, the subspace code size will increase to

$$q^8 - M_1 + \frac{(q^2 + q + 1)M_1}{q^2} = q^8 + \frac{(q + 1)M_1}{q^2}, \quad (1)$$

since new planes contain only q^2 lines disjoint from S . It is clear that M_1 must be a multiple of q^2 , and it has been shown in [21] that $M_1 = q^2$ is not feasible but $M_1 = q^3$ can be realized for a particular choice of \mathcal{L} and as far as only the rearrangement of lines disjoint from S matters. (As an additional requirement, the chosen new planes must not introduce a multiple cover of a line meeting S in a point.) We will now develop the technical machinery needed to derive this result, adapted to the case $v = 7$.

Since the ambient space of $\text{PG}(6, \mathbb{F}_q)$ does not matter (as long as it is 7-dimensional over \mathbb{F}_q), we take it as $V = W \times \mathbb{F}_{q^4}$, where W denotes the trace-zero subspace of $\mathbb{F}_{q^4}/\mathbb{F}_q$ (consisting of all $x \in \mathbb{F}_{q^4}$ satisfying $\text{Tr}(x) = \text{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(x) = x + x^q + x^{q^2} + x^{q^3} = 0$). This allows us to use the additional structure of $\text{PG}(6, \mathbb{F}_q)$ imposed by the extension field \mathbb{F}_{q^4} . In this model our special solid is $S = \{0\} \times \mathbb{F}_{q^4} \cong \mathbb{F}_{q^4}$ (naturally); likewise, we make the identification $W \times \{0\} \cong W$. Subspaces of V/\mathbb{F}_q can be parametrized in the form

$$U = \{(x, f(x) + y); x \in Z, y \in T, f \in \text{Hom}(Z, \mathbb{F}_{q^4}/T)\}, \quad (2)$$

where

$$\begin{aligned} Z &= \{x \in W; \exists y \in \mathbb{F}_{q^4} \text{ such that } (x, y) \in U\}, \\ T &= \{y \in \mathbb{F}_{q^4}; (0, y) \in U\} \end{aligned}$$

and $f: Z \rightarrow \mathbb{F}_{q^4}$ is any \mathbb{F}_q -linear map whose graph (in the sense of Real Analysis) $\Gamma_f = \{(x, f(x)); x \in Z\}$ is contained in U . The \mathbb{F}_q -subspaces $Z \subseteq W$ (projection of U onto W) and $T \subseteq \mathbb{F}_{q^4}$ (naturally isomorphic to the kernel $U \cap S$ of this projection) are uniquely determined by U , while f is only determined up to addition of an \mathbb{F}_q -linear map with values in T and may therefore be replaced by any element in the coset $f + \text{Hom}(Z, T) \in \text{Hom}(Z, \mathbb{F}_{q^4})/\text{Hom}(Z, T) \cong \text{Hom}(Z, \mathbb{F}_{q^4}/T)$.¹⁷ We denote this parametrization by $U = U(Z, T, f)$, using sometimes the

¹⁷It goes without saying that “Hom” denotes the set of \mathbb{F}_q -linear maps between the indicated \mathbb{F}_q -spaces, which forms an \mathbb{F}_q -space of its own with respect to the point-wise operations.

subspaces $Z \times \{0\}$, $\{0\} \times T$ of $\text{PG}(V/\mathbb{F}_q)$ in place of Z, T , as indicated above.

Observe that the subspaces disjoint from S are precisely the graphs $\Gamma_f = U(Z, \{0\}, f)$ of \mathbb{F}_q -linear maps $f: Z \rightarrow \mathbb{F}_{q^4}$. At the other extreme, the subspaces containing S are of the form $U(Z, S, 0) = Z \times S$.

The incidence relation between subspaces of V/\mathbb{F}_q can also be described within this setting: $U(Z', T', f') \subseteq U(Z, T, f)$ if and only if $Z' \subseteq Z$, $T' \subseteq T$ and $f|_{Z'} - f' \in \text{Hom}(Z', T)$.

Now recall from Galois Theory that the powers $\text{id}, \varphi, \varphi^2, \varphi^3$ of the Frobenius automorphism $\varphi: \mathbb{F}_{q^4} \rightarrow \mathbb{F}_{q^4}$, $x \mapsto x^q$ of $\mathbb{F}_{q^4}/\mathbb{F}_q$ form a basis of $\text{End}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ over \mathbb{F}_{q^4} . This says that every \mathbb{F}_q -linear map $f: \mathbb{F}_{q^4} \rightarrow \mathbb{F}_{q^4}$ is evaluation of a unique linearized polynomial $a(X) = a_0X + a_1X^q + a_2X^{q^2} + a_3X^{q^3} \in \mathbb{F}_{q^4}[X]$ of symbolic degree ≤ 3 . For simplicity we write $x \mapsto f(x)$ as $a_0x + a_1x^q + a_2x^{q^2} + a_3x^{q^3}$. The restriction map $f \mapsto f|_W$ then gives that every element of $\text{Hom}(W, \mathbb{F}_{q^4})$ is represented uniquely as $a_0x + a_1x^q + a_2x^{q^2}$ for some $a_0, a_1, a_2 \in \mathbb{F}_{q^4}$ (since the linear maps vanishing on W are of the form $a(x + x^q + x^{q^2} + x^{q^3})$ with $a \in \mathbb{F}_{q^4}$).

Next we name various subspaces of $\text{Hom}(W, \mathbb{F}_{q^4})$, which will subsequently play an important role:

$$\begin{aligned} \mathcal{G} &= \{a_0x + a_1x^q; a_0, a_1 \in \mathbb{F}_{q^4}\}, \\ \mathcal{R} &= \{ax^q - a^qx; a \in \mathbb{F}_{q^4}\}, \\ \mathcal{T} &= \{ax^q - a^qx; a \in W\}, \\ \mathcal{D}(Z, P) &= r(ab^q - a^qb)^{-1} \langle ax^q - a^qx, bx^q - b^qx \rangle \end{aligned}$$

for a 2-dimensional subspace $Z = \langle a, b \rangle$ of W and a point $P = \mathbb{F}_q(0, r)$ of the special solid S (i.e. $r \in \mathbb{F}_{q^4}^\times$). The space \mathcal{G} has minimum rank distance 2 (since $a_0x + a_1x^q \neq 0$ has at most q zeros in W) and size $\#\mathcal{G} = q^8$. It is therefore an MRD code. We call it the *Gabidulin code*, since it is a basis-free version of a member of the family of MRD codes constructed in [18], which are nowadays commonly called Gabidulin codes. Further we have $\mathcal{D}(Z, P) \subset \mathcal{T} \subset \mathcal{R} \subset \mathcal{G}$, \mathcal{T} has constant rank 2 (since $ax^q - a^qx$ has 1-dimensional kernel \mathbb{F}_qa if $a \in W \setminus \{0\}$), $\mathcal{R} \setminus \mathcal{T}$ has constant rank 3, and $\mathcal{D}(Z, P)$ consists of all linear maps $f \in \mathcal{G}$ satisfying $f(Z) \subseteq \mathbb{F}_qr$.¹⁸

Finally we fix $\mathcal{L} = \{\Gamma_f; f \in \mathcal{G}\}$ for the remainder of this article and call \mathcal{L} the *lifted Gabidulin code*. The reader may check that $f \mapsto \Gamma_f$ provides a basis-free description of the lifting construction (passing from matrix codes to subspace codes) and hence \mathcal{L} is a plane LMRD code as needed for the subsequent discussion.

¹⁸Of course $0 \in \mathcal{T}$ has rank $0 \neq 2$, but it is custom to refer to a matrix space as a constant-rank space if all nonzero matrices in the matrix space have the same rank.

Lemma 4. *For a set of planes $\mathcal{L}_1 \subseteq \mathcal{L}$ let $\mathcal{G}_1 \subseteq \mathcal{G}$ be the corresponding set of linear maps in the Gabidulin code. In order that the free lines determined by \mathcal{L}_1 can be rearranged into new planes meeting S in a point, it is necessary and sufficient that $\#\mathcal{G}_1 = mq^2$ is a multiple of q^2 and for each 2-dimensional subspace $Z \subset W$ there exist (not necessarily distinct) points P_1, \dots, P_m on S and linear maps $f_1, \dots, f_m \in \mathcal{G}$ such that*

$$\mathcal{G}_1 = \biguplus_{i=1}^m (f_i + \mathcal{D}(Z, P_i)).$$

Note that the condition requires \mathcal{G}_1 to be a union of cosets of spaces $\mathcal{D}(Z, P)$ simultaneously in $q^2 + q + 1$ different ways, one for each 2-dimensional subspace $Z \subset W$. The number of new planes in the rearrangement must be $m(q^2 + q + 1)$, but the rearrangement itself is perhaps not uniquely determined by \mathcal{G}_1 . Moreover, the lemma does not say anything about whether the rearrangement introduces a multiple cover of some line meeting S in a point.

Proof of the lemma. Lines L disjoint from S as well as new planes N meeting S in a point are contained in a unique hyperplane H above S ($H = L + S$ resp. $H = N + S$). “Old” planes $E \in \mathcal{L}$ are transversal to these hyperplanes and the H -section $E \mapsto E \cap H$ identifies \mathcal{L} with the set of q^8 lines in $\text{PG}(H)$ disjoint from S (since \mathcal{L} is an LMRD code). In terms of the parametrization $H = H(Z, \mathbb{F}_{q^4}, 0)$, $E = \Gamma_f$, $L = \Gamma_g$ the corresponding H -section is just restriction $g = f|_Z$. Thus we can look at each hyperplane above S separately.

Let H be such a hyperplane and Z the corresponding 2-dimensional subspace of W . Planes in H meeting S in the point $P = \mathbb{F}_q(0, r)$ have the form $N = N(Z, \mathbb{F}_q r, g)$ with $g \in \text{Hom}(Z, \mathbb{F}_{q^4})$ and contain the q^2 lines $L = \Gamma_h$, $h \in g + \text{Hom}(Z, \mathbb{F}_q r)$, disjoint from S . Denoting by $f \in \mathcal{G}$ the unique linear map such that $f|_Z = g$, we have that $f + \mathcal{D}(Z, P)$ restricts to $g + \text{Hom}(Z, \mathbb{F}_q r)$ on Z . Hence the mq^2 free lines in H determined by the planes in \mathcal{L}_1 can be rearranged into new planes $N(Z, \mathbb{F}_q r, g)$ iff \mathcal{G}_1 is a disjoint union of cosets of the form $f + \mathcal{D}(Z, P)$ with $P \in S$, $f \in \mathcal{G}_1$. \square

Now observe that our distinguished space \mathcal{T} contains one space $\mathcal{D}(Z, P)$ for each $Z = \langle a, b \rangle \subset W$, viz. $\mathcal{D}(Z, P)$ with $P = \mathbb{F}_q(0, ab^q - a^q b)$. Hence $\mathcal{G}_1 = \mathcal{T}$ satisfies the conditions of Lemma 4 with $m = q$, $P_1 = \dots = P_q = P = \mathbb{F}_q(0, ab^q - a^q b)$ and f_1, \dots, f_q a system of coset representatives for $\mathcal{T}/\mathcal{D}(Z, P)$. A fortiori the same is true for any coset of \mathcal{T} in \mathcal{G} , and even for any disjoint union of “rotated” cosets $\biguplus_{j=1}^r (f_j + r_j \mathcal{T})$ with $r_j \in \mathbb{F}_{q^4}^\times$ and $f_j \in \mathcal{G}$.¹⁹

The next theorem, which closes this section, shows that if we take $\mathcal{G}_1 = \mathcal{R}$, the distinguished subspace of order q^4 defined along with

¹⁹For the latter the points P_i vary not only with Z but also with j .

\mathcal{T} , then the corresponding rearrangement into new planes does not introduce a multiple line cover and hence results in a plane subspace code with $t = 2$.

Theorem 2. *Let \mathcal{C} be the set of planes in $\text{PG}(W \times \mathbb{F}_{q^4}) \cong \text{PG}(6, \mathbb{F}_q)$ obtained by removing all planes $E = \Gamma_f$, $f \in \mathcal{R}$, from \mathcal{L} and adding all planes of the form $N = N(Z, P, g)$ with $Z = \langle a, b \rangle \subset W$ 2-dimensional, $P = \mathbb{F}_q(0, ab^q - a^q b)$ (so P depends on Z) and $g = f|_Z$ for some $f \in \mathcal{R}$. Then \mathcal{C} forms a subspace code (i.e., $t = 2$) of size $\#\mathcal{C} = q^8 + q^3 + q^2$. Moreover, \mathcal{C} can be augmented by $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$ further planes meeting S in a line to a subspace code $\hat{\mathcal{C}}$ of size $\#\hat{\mathcal{C}} = q^8 + q^4 + 2q^3 + 3q^2 + q + 1$.*

Proof. Since $M_1 = \#\mathcal{R} = q^4$, the rearrangement increases the size of the subspace code by $(q+1)M_1/q^2 = q^3 + q^2$. Thus $\#\mathcal{C} = q^8 + q^3 + q^2$, and it remains to show that \mathcal{C} still has $t = 2$.

By Lemma 4 and the definition of \mathcal{C} , the new planes $N = N(Z, P, g)$ added to $\mathcal{L}_0 = \mathcal{L} \setminus \mathcal{L}_1$ cover each free line exactly once. Hence it suffices to check that no line meeting S in a point is covered more than once.

To this end we first show that the map $\langle a, b \rangle \mapsto \mathbb{F}_q(ab^q - a^q b)$ (i.e. $Z \mapsto P$) is one-to-one. This implies that new planes in different hyperplanes above S do not meet on S and hence cannot intersect in a line. Suppose, by contradiction, that different subspaces Z_1, Z_2 of W correspond to the same point P . Since $\dim(Z_1 \cap Z_2) = 1$, we can write $Z_1 = \langle a, b_1 \rangle$, $Z_2 = \langle a, b_2 \rangle$. The \mathbb{F}_q -linear map $ax^q - a^q x \in \text{Hom}(W, \mathbb{F}_{q^4})$ has kernel $\mathbb{F}_q a$ and hence maps Z_1, Z_2 to different 1-dimensional subspaces $\mathbb{F}_q(ab_1^q - a^q b_1) \neq \mathbb{F}_q(ab_2^q - a^q b_2)$; contradiction!

Next let $N_1 = N(Z, P, g_1)$, $N_2 = N(Z, P, g_2)$, $g_i = f_i|_Z$, be different new planes meeting S in the same point P (and hence with the same Z). Write $Z = \langle a, b \rangle$ and $f_1(x) - f_2(x) = u_0 x + u_1 x^q$. The planes N_1, N_2 have a point outside S (and hence a line through P) in common iff there exists $x \in Z \setminus \{0\}$ such that $f_1(x) - f_2(x) \in \mathbb{F}_q(ab^q - a^q b)$. Setting $x = \lambda a + \mu b$, this is equivalent to a nontrivial solution $(\lambda, \mu, \nu) \in \mathbb{F}_q^3$ of the equation

$$\lambda(u_0 a + u_1 a^q) + \mu(u_0 b + u_1 b^q) + \nu(ab^q - a^q b) = 0.$$

Thus $f_1, f_2 \in \mathcal{G}$ determine new planes N_1, N_2 satisfying $N_1 \cap N_2 = \{P\}$ for those choices of $Z = \langle a, b \rangle \subset W$ (equivalently, for those choices of the hyperplane $H = Z + S$) for which $u_0 a + u_1 a^q, u_0 b + u_1 b^q, ab^q - a^q b$ are linearly independent over \mathbb{F}_q .²⁰

With these preparations we can now prove that \mathcal{C} still has $t = 2$. For $f_1, f_2 \in \mathcal{R}$ we have $f_1 - f_2 \in \mathcal{R}$ and hence of the form $ux^q - u^q x$. If f_1, f_2 are in different cosets of $\mathcal{D}(Z, P)$ then $u \notin Z$. The equation

²⁰Viewed projectively, this requires that $f(x) = u_0 x + u_1 x^q$ maps the line $Z = \langle a, b \rangle$ to another line $Z' = f(Z)$ of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ and the point $\mathbb{F}_q(ab^q - a^q b)$ corresponding to Z is not on Z' .

$\lambda(ua^q - u^qa) + \mu(ub^q - u^qb) + \nu(ab^q - a^qb) = 0$ can be rewritten as

$$\begin{vmatrix} a & b & u \\ a^q & b^q & u^q \\ -\mu & \lambda & \nu \end{vmatrix} = 0.$$

If (λ, μ, ν) is nonzero then using the linear dependence of the rows of this matrix we can express the conjugates $(a^{q^i}, b^{q^i}, u^{q^i})$ as linear combinations (with coefficients in \mathbb{F}_{q^4}) of (a, b, u) and $(-\mu, \lambda, \nu) \in \mathbb{F}_q^3$. This shows that the 4×3 matrix formed from the conjugates of (a, b, u) has rank 2 and implies that a, b, u are linearly dependent over \mathbb{F}_q ; contradiction. Thus \mathcal{C} has the required property.

The augmented subspace code $\widehat{\mathcal{C}}$ is constructed in the same way as in the proof of Theorem 1. The only thing that needs to be checked is that each 4-flat F above S contains a point $Q \notin S$ that is not covered by any new plane $N \in \mathcal{C}$. Equivalently, for any $x \in W \setminus \{0\}$ the new planes $N = N(Z, \mathbb{F}_q r, g)$ with $x \in Z$ do not cover all q^4 points $\mathbb{F}_q(x, y)$, $y \in \mathbb{F}_{q^4}$. This property will now be verified through explicit computation.

A 2-dimensional subspace $Z \subset W$ containing x has the form $Z = \langle a, x \rangle$ with $a \in W$ and $ax^q - a^qx \neq 0$. The points $\mathbb{F}_q(x, y)$ covered by the q^2 new planes corresponding to Z have $y = ux^q - u^qx + \mu(ax^q - a^qx) = (u + \mu a)x^q - (u + \mu a)^qx$ for $u \in \mathbb{F}_{q^4}/Z$, $\mu \in \mathbb{F}_q$. It follows that y takes precisely the q^3 values in the image I of the linear map $c \mapsto cx^q - c^qx$, which has kernel $\mathbb{F}_q x$. In other words, the points in the 4-flat $F = (\mathbb{F}_q x) \times S$ covered by the new planes in \mathcal{C} form the affine part of a solid, viz. $(F_q x) \times I$, with plane at infinity $\{0\} \times I$. In particular, there are $q^4 - q^3$ valid choices for the point Q . This completes the proof of the Theorem 2. \square

In the binary case $q = 2$ the size of the augmented subspace code in Theorem 2 is $\#\widehat{\mathcal{C}} = 303$, falling short by 1 of the corresponding code in [26]. On the other hand, $\#\widehat{\mathcal{C}}$ strictly exceeds the bound imposed on codes containing an LMRD code for every q , showing already the effectiveness of our approach. However, this is not the end of the story; Theorem 2 will be improved upon later.

5. AN ATTEMPT TO CONSTRUCT A q -ANALOGUE AND ITS FAILURE

In this section we apply the method developed in the previous section to the construction problem for q -analogues of the Fano plane. The attempt eventually fails for every q but produces the largest known plane subspace codes in $\text{PG}(6, \mathbb{F}_q)$.

We start with a few words on automorphisms of subspace codes in $\text{PG}(V/\mathbb{F}_q)$. The group $G = \text{GL}(V/\mathbb{F}_q)$ obviously acts on plane subspace codes in $\text{PG}(V/\mathbb{F}_q)$, but is by way too large for our purpose. The stabilizer G_S of our special solid S in $\text{GL}(V/\mathbb{F}_q)$ consists of all maps L

of the form $(x, y)L = (xL_{11}, xL_{12} + yL_{22})$ with $L_{11} \in \text{GL}(W/\mathbb{F}_q)$, $L_{22} \in \text{GL}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ and $L_{12} \in \text{Hom}(W, \mathbb{F}_{q^4})$. The map L sends a plane $E = \Gamma_f$ disjoint from S to Γ_g with $g = L_{11}^{-1}fL_{22} + L_{11}^{-1}L_{12}$ (composition of maps is from left to right for the moment), so that on the corresponding maps $f \in \text{Hom}(W, \mathbb{F}_{q^4})$ it affords the group of all “affine” transformations $f \mapsto A \circ f \circ B + C$ with $A \in \text{GL}(\mathbb{F}_{q^4}/\mathbb{F}_q)$, $B \in \text{GL}(W/\mathbb{F}_q)$ and $C \in \text{Hom}(W, \mathbb{F}_{q^4})$.

The group G_S is still too large for our purpose, but we have that the Gabidulin code \mathcal{G} is invariant under the subgroup consisting of all maps $f \mapsto rf$ with $r \in \mathbb{F}_{q^4}^\times$, which acts as a Singer group on the projective space $\text{PG}(S/\mathbb{F}_q) \cong \text{PG}(3, \mathbb{F}_q)$. This group, or rather the corresponding subgroup $\Sigma \leq \text{GL}(V/\mathbb{F}_q)$ consisting of all maps $(x, y) \mapsto (x, ry)$ with $r \in \mathbb{F}_{q^4}^\times$, is suitable for our purpose.²¹ It is our next goal to make the expurgation-augmentation process of Section 4 invariant under Σ .

How large should the set \mathcal{L}_1 of removed planes be for a putative q -analogue \mathcal{F}_q ? We can arrange coordinates in such a way that S does not contain a block of \mathcal{F}_q and hence $q^8 - q^7 + q^3$ blocks are disjoint from S ; cf. Lemma 2. This requires

$$\#\mathcal{L}_1 = q^7 - q^3 = q^3(q^4 - 1) = (q^4 - q^3)(q^3 + q^2 + q + 1)$$

and the number of new planes through each point $P \in S$ to be $(q^4 - q^3)(q^2 + q + 1)/q^2 = q^4 - q$.²² Hence a Σ -invariant construction of \mathcal{F}_q is at least conceivable and, even better, there is a canonical candidate for a Σ -invariant subset $\mathcal{G}_1 \subset \mathcal{G}$ of the appropriate size, viz. the union of all “rotated” cosets $r(f + \mathcal{T})$ with $f \in \mathcal{R} \setminus \mathcal{T}$ and $r \in \mathbb{F}_{q^4}^\times$.²³ A moment’s reflection shows that this set \mathcal{G}_1 consists precisely of all binomials $a_0x + a_1x^q$ with 1-dimensional kernel in $\mathbb{F}_{q^4}/\mathbb{F}_q$ complementary to W (thus the rank in $\text{Hom}(W, \mathbb{F}_{q^4})$ is 3). The complementary subset $\mathcal{G}_0 = \mathcal{G} \setminus \mathcal{G}_1$ consists of 0, the $2(q^4 - 1)$ monomials rx, rx^q with $r \in \mathbb{F}_{q^4}^\times$, the $(q^4 - 1)(q^2 + q + 1)$ binomials $r(ux^q - u^qx)$ with $r \in \mathbb{F}_{q^4}^\times$ and $u \in W \setminus \{0\}$ (these have rank 2 in $\text{Hom}(W, \mathbb{F}_{q^4})$) and $(q^4 - 1)(q^3 + q^2 + q + 1)(q - 2)$ binomials $a_0x + a_1x^q$ with no nontrivial zero in \mathbb{F}_{q^4} . The set \mathcal{G}_1 decomposes as

$$\mathcal{G}_1 = \biguplus_{r \in \mathbb{F}_{q^4}^\times / \mathbb{F}_q^\times} r(\mathcal{R} \setminus \mathcal{T}),$$

showing that the $(q - 1) \times \frac{q^4 - 1}{q - 1} = q^4 - 1$ cosets $r(f + \mathcal{T})$ used are pairwise disjoint, as needed for the construction.

²¹Viewed as collineation group, Σ has order $q^4 - 1$ (not the same as the Singer group).

²²As a consistency check, use that this number can also be obtained by subtracting from the total number $q^4 + q^2 + 1$ of blocks through P (cf. Lemma 2) the number $q^2 + q + 1$ of blocks that meet S in a line through P . Indeed, $q^4 + q^2 + 1 - (q^2 + q + 1) = q^4 - q$.

²³The spaces $r\mathcal{T}$ itself cannot be used, since these are not disjoint.

New planes are defined by connecting the free lines L in the planes corresponding to $f + \mathcal{T}$ to the points $P = \mathbb{F}_q(0, ab^q - a^qb)$, where $Z = \langle a, b \rangle \subset W$ is the 2-dimensional subspace determined by the hyperplane $H = L + S = Z \times S$ (the same definition as in Section 4), and rotating: Free lines in the planes corresponding to $r(f + \mathcal{T})$, $r \in \mathbb{F}_{q^4}^\times$, are connected to $rP = \mathbb{F}_q(0, r(ab^q - a^qb))$ in the same way. The collection \mathcal{N} of $(q^4 - q)(q^3 + q^2 + q + 1)$ new planes determined in this way is certainly Σ -invariant and contains $q^4 - q$ planes meeting S in any particular point P . By construction, \mathcal{N} forms an exact cover of the free lines determined by \mathcal{L}_1 (and $\mathcal{L}_0 \cup \mathcal{N}$ forms an exact cover of all lines disjoint from S), but \mathcal{N} may cover some lines meeting S in a point more than once.

If for some value of q the set $\mathcal{L}_0 \cup \mathcal{N}$ still had $t = 2$, then the present construction would have been a big step towards the desired q -analogue \mathcal{F}_q , leaving only the task to augment it by $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q$ further planes meeting S in a line. Unfortunately, however, it turns out that $\mathcal{L}_0 \cup \mathcal{N}$ never has $t = 2$, rendering a construction of a q -analogue \mathcal{F}_q in this way impossible. This negative result will follow from our subsequent analysis, which on the other hand will tell us precisely how many planes should be removed from $\mathcal{L}_0 \cup \mathcal{N}$ in order to restore $t = 2$. Fortunately, this number turns out to be rather small.

Let $\mathcal{N}_1 \subset \mathcal{N}$ be the set of $q^4 - q = (q - 1)(q^3 + q^2 + q)$ new planes passing through the special point $P_1 = \mathbb{F}_q(0, 1)$. We are interested in finding the largest subset(s) $\mathcal{N}'_1 \subseteq \mathcal{N}_1$ consisting of planes mutually intersecting in P_1 . Denoting by M'_1 the maximum size of such a subset \mathcal{N}'_1 , it is clear from the preceding development and Σ -invariance of \mathcal{N} that \mathcal{L}_0 can then be augmented by a subset \mathcal{N}' of size $M' = M'_1(q^3 + q^2 + q + 1)$ without increasing t . If \mathcal{N}'_1 is invariant under the subgroup of Σ corresponding to \mathbb{F}_q^\times then \mathcal{N}' may be taken in the form $\mathcal{N}' = \biguplus_{L \in \Sigma} L(\mathcal{N}'_1) = \biguplus_{r \in \mathbb{F}_{q^4}^\times / \mathbb{F}_q^\times} r\mathcal{N}'_1$, making the augmented subspace code $\mathcal{C} = \mathcal{L}_0 \cup \mathcal{N}'$ again Σ -invariant.²⁴ If \mathcal{N}'_1 is not uniquely determined then there are many further choices for \mathcal{N}' , which could lead to better overall subspace codes during the final augmentation step.²⁵

Before writing down \mathcal{N}_1 in explicit form we will introduce some further terminology. Relative to a 2-dimensional subspace $Z \subset W$, the letters a, b, c, d will henceforth denote a basis of $\mathbb{F}_{q^4}/\mathbb{F}_q$ such that $Z = \langle a, b \rangle$, $W = \langle a, b, c \rangle$ and $\text{Tr}(d) = 1$.²⁶ Further we set $\delta(x, y) = xy^q - x^qy = \begin{vmatrix} x & y \\ x^q & y^q \end{vmatrix}$ for $x, y \in \mathbb{F}_{q^4}$, which constitutes an \mathbb{F}_q -bilinear, antisymmetric map with right annihilators $\{y \in \mathbb{F}_{q^4}; \delta(x, y) = 0\} = \mathbb{F}_q x$

²⁴“ $r\mathcal{N}'_1$ ” refers to the image of \mathcal{N}'_1 under $(x, y) \mapsto (x, ry)$.

²⁵Later we will see that the number of choices for \mathcal{N}'_1 is at least $(q^2)^{q^3+q^2+q+1}$; cf. Section 6.

²⁶The element d can be fixed once and for all, but c depends on Z , of course.

and corresponding right images $\delta(x, \mathbb{F}_{q^4}) = \{z \in \mathbb{F}_{q^4}; \text{Tr}(x^{-q-1}z) = 0\} = x^{q+1}W$ (provided that $x \neq 0$). The latter follows from Hilbert's Satz 90, using $z = xy^q - x^qy \iff x^{-q-1}z = (y/x)^q - y/x$. Since $\delta(x, y) = x \prod_{\lambda \in \mathbb{F}_q} (y - \lambda x)$, we also have that $\mathbb{F}_q \delta(x, y)$ depends only on the line $L = \langle x, y \rangle$ of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ (provided that $\mathbb{F}_q x \neq \mathbb{F}_q y$) and is computed as the product of all points of L in $\mathbb{F}_{q^4}^\times/\mathbb{F}_q^\times$. Accordingly, we can write $\delta(L)$ for $\mathbb{F}_q \delta(x, y)$ and thus have a well-defined map $L \mapsto \delta(L)$ from lines to points of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$. As shown above, $L \mapsto \delta(L)$ maps the line pencil through $\mathbb{F}_q x$ bijectively onto the plane $x^{q+1}W$,²⁷ but we also have the following

Lemma 5. *$L \mapsto \delta(L)$ maps the lines contained in any plane E of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ bijectively onto the points of another plane E' . If $\epsilon \in \mathbb{F}_{q^4}^\times$ satisfies $\epsilon^q = -\epsilon$ then $(aW)' = a^{q+1}\epsilon W$ for $a \in \mathbb{F}_{q^4}^\times$.*

Note that $\epsilon^q = -\epsilon$, or $\epsilon^{q-1} = -1$, is equivalent to $\epsilon \in \mathbb{F}_q^\times$ for even q and to $\epsilon \notin \mathbb{F}_q^\times \wedge \epsilon^2 \in \mathbb{F}_q^\times$ for odd q . In the latter case $\mathbb{F}_q^\times \epsilon$ is the unique element of order 2 in $\mathbb{F}_{q^4}^\times/\mathbb{F}_q^\times$. Further note that every plane of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ has the form aW for some $a \in \mathbb{F}_{q^4}^\times$ (by Singer's Theorem).

Proof. Since any two lines in E intersect and $L \mapsto \delta(L)$ is injective on line pencils, it is clear that the $q^2 + q + 1$ points $\delta(L)$ for $L \subset E$ are distinct.

Now consider the special plane $E = W = \{x \in \mathbb{F}_{q^4}; x + x^q + x^{q^2} + x^{q^3} = 0\}$. For $x, y \in W$ we have

$$\begin{aligned} \text{Tr}(\epsilon \delta(x, y)) &= \text{Tr}(\epsilon xy^q - \epsilon x^q y) \\ &= \epsilon xy^q - \epsilon x^q y^{q^2} + \epsilon x^{q^2} y^{q^3} - \epsilon x^{q^3} y - (\epsilon x^q y - \epsilon x^{q^2} y^q + \epsilon x^{q^3} y^{q^2} - \epsilon xy^{q^3}) \\ &= \epsilon(x + x^{q^2})(y^q + y^{q^3}) - \epsilon(x^q + x^{q^3})(y + y^{q^2}) \\ &= \epsilon(x + x^{q^2})(y^q + y^{q^3}) + \epsilon(x + x^{q^2})(y + y^{q^2}) \\ &= \epsilon(x + x^{q^2})(y + y^q + y^{q^2} + y^{q^3}) = 0 \end{aligned}$$

and hence $\delta(x, y) \in \epsilon^{-1}W = \epsilon W$. Thus $W' = \epsilon W$, and then $\delta(ax, ay) = a^{q+1}\delta(x, y)$ yields $(aW)' = a^{q+1}\epsilon W$. \square

Finally, for a plane E in $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ we define $\delta(E)$ as the product of all points on E in $\mathbb{F}_{q^4}^\times/\mathbb{F}_q^\times$ (this yields a map $E \mapsto \delta(E)$ from planes to points of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ and is completely analogous to the case of lines), and in the case $E \neq W$ another projective invariant $\sigma(E)$ as

$$\sigma(E) = \frac{\delta(E)}{\delta(Z)^{q+1}}, \quad \text{where } Z = E \cap W. \quad (3)$$

²⁷This fact was already used implicitly in some proofs.

The reason for this extra definition will become clear in a moment (cf. the subsequent Lemma 6).

Now we turn to the description of the new planes in \mathcal{N}_1 . By the reasoning in Section 4 and since $\mathcal{D}(Z, P_1) = \mathcal{D}(\langle a, b \rangle, P_1) = \delta(a, b)^{-1} \langle ax^q - a^q x, bx^q - b^q x \rangle$, the planes in \mathcal{N}_1 are parametrized as $N = N(Z, P_1, g)$, where $Z \subset W$ is 2-dimensional and $g: Z \rightarrow \mathbb{F}_{q^4}$ is of the form

$$g(x) = \delta(a, b)^{-1} (\lambda(dx^q - d^q x) + \mu(cx^q - c^q x)) = \frac{\delta(\lambda d + \mu c, x)}{\delta(a, b)}$$

with $\lambda \in \mathbb{F}_q^\times$, $\mu \in \mathbb{F}_q$ ($q^4 - q$ choices for N), and cover the $(q+1)q$ points

$$\mathbb{F}_q \left(x, \frac{\delta(\lambda d + \mu c, x)}{\delta(a, b)} + \nu \right), \quad \mathbb{F}_q x \in Z, \nu \in \mathbb{F}_q \quad (4)$$

outside S .

We call a pair of new planes $N, N' \in \mathcal{N}_1$ a *collision* if N, N' have a point outside S (and hence a line through P_1) in common. Such collisions are precisely the obstructions to adding N, N' simultaneously to the expurgated LMRD code $\mathcal{L}_0 = \mathcal{L} \setminus \mathcal{L}_1$ of size $q^8 - q^7 + q^3$. From Theorem 2 (and its “rotated” analogues, so-to-speak) we know that collisions between $N = N(Z, P_1, g)$ and $N' = N(Z', P_1, g')$ can occur only if $Z \neq Z'$. In this case $Z \cap Z' = \mathbb{F}_q z$ is a single point, so that every collision takes the form

$$\frac{\delta(\lambda d + \mu c, z)}{\delta(a, z)} + \nu = \frac{\delta(\lambda' d + \mu' c, z)}{\delta(a', z)} + \nu' \quad (5)$$

with z, a, a' spanning W . Rewriting the denominator as $\delta(a, z)$ makes the actual correspondence $(Z, \lambda, \mu) \mapsto N$ depend on z . However, since $\delta(a, b)$ and $\delta(a, z)$ differ only by a factor in \mathbb{F}_q^\times , this dependence disappears in the projective view, where Z and the point $\mathbb{F}_q(\lambda d + \mu c)$ correspond collectively to a set of $q-1$ new planes, viz. $N(Z, P_1, \mathbb{F}_q^\times g)$ with $g(x) = \delta(\lambda d + \mu c, x)/\delta(a, b)$.²⁸

Further note that setting $E = Z + \mathbb{F}_q(\lambda d + \mu c)$ gives a parametrization of the $q^4 - q = (q-1)(q^3 + q^2 + q)$ new planes in \mathcal{N}_1 , $q-1$ planes at a time, by the $q^3 + q^2 + q$ planes $E \neq W$ of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$.²⁹

Lemma 6. *Let $N = N(Z, P_1, g)$, $N' = N(Z', P_1, g')$ be planes in \mathcal{N}_1 parametrized by distinct planes E, E' of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ in the fashion just described. Collisions between any of the $2(q-1)$ planes in $N(Z, P_1, \mathbb{F}_q^\times g) \uplus N(Z', P_1, \mathbb{F}_q^\times g')$ fall into the following two cases:*

- (i) $\sigma(E) \neq \sigma(E')$. In this case there are no collisions among the planes in $N(Z, P_1, \mathbb{F}_q^\times g) \uplus N(Z', P_1, \mathbb{F}_q^\times g')$.

²⁸Of course this remark also applies when changing the generators a, b of Z .

²⁹Since the line $\langle c, d \rangle$ is skew to Z , the q points $\mathbb{F}_q(d + \mu c)$, $\mu \in \mathbb{F}_q$, determine the q planes $E \neq W$ above Z . Replacing $\lambda d + \mu c$ by $\lambda d + \mu c + \alpha a + \beta b$ has no effect on the plane $N(Z, P_1, g)$, since $\delta(a, x), \delta(b, x) \in \mathbb{F}_q \delta(Z)$ for $x \in Z$ and hence g is only changed inside the coset $g + \text{Hom}(Z, \mathbb{F}_q)$.

- (ii) $\sigma(E) = \sigma(E')$. In this case any new plane in $N(Z, P_1, \mathbb{F}_q^\times g)$ collides with a unique new plane in $N(Z', P_1, \mathbb{F}_q^\times g')$ and vice versa, and we can select a maximum of $q - 1$ mutually non-colliding planes from $N(Z, P_1, \mathbb{F}_q^\times g) \uplus N(Z', P_1, \mathbb{F}_q^\times g')$.

Proof. First suppose $Z = Z'$. In this case there are no collisions, and we must show $\sigma(E) \neq \sigma(E')$ or, equivalently, $\delta(E) \neq \delta(E')$. The planes of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ have the form rW with r running through a system of coset representatives for \mathbb{F}_q^\times in $\mathbb{F}_{q^4}^\times$, and clearly $\delta(rW) = r^{q^2+q+1}\delta(W)$. Since $\gcd(q^3 + q^2 + q + 1, q^2 + q + 1) = 1$, $E \mapsto \delta(E)$ is a bijection and the result follows.

Now suppose $Z \neq Z'$ and set $Z \cap Z' = \mathbb{F}_q z$. Assuming w.l.o.g. $g(x) = \delta(d + \mu c, x)/\delta(a, x)$, we have from (4) that the points on $N(Z, P_1, \lambda g)$ of the form $\mathbb{F}_q(z, y)$ are those with $y \in \lambda g(z) + \mathbb{F}_q$, i.e. the q points $\neq P_1$ on the line through $\mathbb{F}_q(z, \lambda g(z))$ and P_1 . Hence the points $\mathbb{F}_q(z, y)$ on the planes in $N(Z, P_1, \mathbb{F}_q^\times g)$ are those with $y \in \mathbb{F}_q^\times g(z) + \mathbb{F}_q$, an orbit of the affine group $\text{AGL}(1, \mathbb{F}_q) = \{u \mapsto \lambda u + \nu; \lambda \in \mathbb{F}_q^\times, \nu \in \mathbb{F}_q\}$ acting on \mathbb{F}_{q^4} . The orbits corresponding to N, N' are either disjoint and there are no collisions, or the orbits coincide and the planes in $N(Z, P_1, \mathbb{F}_q^\times g)$ and $N(Z', P_1, \mathbb{F}_q^\times g')$ are matched up in pairs covering the same line L through P_1 and a point of the form $\mathbb{F}_q(z, \lambda g(z))$. In this case we can select at most one plane from each matching pair without introducing collisions. If we do so, the selected planes will cover the same lines L as the corresponding planes in $N(Z, P_1, \mathbb{F}_q^\times g)$, say, and hence there is no obstruction to selecting exactly one plane from each pair.

It remains to show that the two cases just described are characterized by $\sigma(E) \neq \sigma(E')$ and $\sigma(E) = \sigma(E')$, respectively. For this we use the fact that $\mathbb{F}_q^\times u_1 + \mathbb{F}_q = \mathbb{F}_q^\times u_2 + \mathbb{F}_q$, or $\mathbb{F}_q u_1 + \mathbb{F}_q = \mathbb{F}_q u_2 + \mathbb{F}_q$, is equivalent to $\mathbb{F}_q(u_1^q - u_1) = \mathbb{F}_q(u_2^q - u_2)$. This is an instance of the equivalence $\delta(L_1) = \delta(L_2) \iff L_1 = L_2$ for lines L_1, L_2 through the same point (in this case the point $\mathbb{F}_q = \mathbb{F}_q 1$).³⁰ Using this fact and

³⁰It is also straightforward to show directly that $u \mapsto (u^q - u)^{q-1}$ is a separating invariant for the orbits of $\text{AGL}(1, \mathbb{F}_q)$ on \mathbb{F}_{q^4} , i.e. $\mathbb{F}_q^\times u_1 + \mathbb{F}_q = \mathbb{F}_q^\times u_2 + \mathbb{F}_q$ iff $(u_1^q - u_1)^{q-1} = (u_2^q - u_2)^{q-1}$.

$u^q - u = \prod_{\lambda \in \mathbb{F}_q} (u + \lambda)$ we can rewrite the collision criterion (5) as

$$\begin{aligned}
g(z)^q - g(z) &= \prod_{\nu \in \mathbb{F}_q} \frac{\delta(d + \mu c, z) + \nu \delta(a, z)}{\delta(a, z)} \\
&= \delta(a, z)^{-q} \prod_{\nu \in \mathbb{F}_q} \delta(d + \mu c + \nu a, z) \\
&\in \delta(Z)^{-q} \prod_{\substack{L \subset E \\ \mathbb{F}_q z \in L \wedge L \neq Z}} \delta(L) \\
&= \delta(Z)^{-q-1} \prod_{\substack{L \subset E \\ \mathbb{F}_q z \in L}} \delta(L) \\
&= \frac{\delta(E)}{\delta(Z)^{q+1}} \cdot (\mathbb{F}_q z)^q \\
&= \sigma(E) \cdot (\mathbb{F}_q z)^q = \sigma(E') \cdot (\mathbb{F}_q z)^q,
\end{aligned}$$

where we have used that the product of all points in E on the $q + 1$ lines through $\mathbb{F}_q z$ involves $\mathbb{F}_q z$ exactly $q + 1$ times and all other points exactly once. Cancelling the factor $(\mathbb{F}_q z)^q$ completes the proof of the lemma. \square

As a consequence of Lemma 6 we obtain that there exist subsets $\mathcal{N}'_1 \subseteq \mathcal{N}_1$ of size $\#\mathcal{N}'_1 = (q - 1) \cdot \#\text{Im}(\sigma)$ which can be added to the expurgated LMRD code \mathcal{L}_0 while still maintaining $t = 2$. For this we choose for each point Q in the image of σ a plane $E \neq W$ with $\sigma(E) = Q$ and take \mathcal{N}'_1 as the union of all sets $N(Z, P_1, \mathbb{F}_q^\times g)$ parametrized by these planes. In the smallest case $q = 2$, where $\#N(Z, P_1, \mathbb{F}_q^\times g) = 1$, such a set \mathcal{N}'_1 is clearly maximal.³¹

Hence our next goal is to obtain more detailed information on the map $E \mapsto \sigma(E)$ with domain the set of $q^3 + q^2 + q$ planes $E \neq W$ in $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$, and in particular determine its image size. As a first step towards this we establish an explicit formula for $\sigma(E)$. The formula is stated in terms of the absolute invariant $\sigma(E)^{q-1} \in \mathbb{F}_{q^4}^\times$, which is obtained by composing $E \mapsto \sigma(E)$ with the group isomorphism $\mathbb{F}_{q^4}^\times/\mathbb{F}_q^\times \rightarrow (\mathbb{F}_{q^4}^\times)^{q-1}$, $r\mathbb{F}_q^\times \mapsto r^{q-1}$.

Lemma 7. *For a plane $E = aW \neq W$ of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ we have*

$$\sigma(E)^{q-1} = 1 - \frac{a^{(q-1)(q^2+1)} - 1}{a^{q-1} - 1}.$$

Proof. First we show $\delta(W) = \mathbb{F}_q \epsilon$ or, equivalently, $\delta(W)^{q-1} = -1$, with ϵ as in Lemma 5. From $X^{q^3} + X^{q^2} + X^q + X = \prod_{w \in W} (X - w)$ the product of all elements in $W \setminus \{0\}$ is 1. For a point $P = \mathbb{F}_q x$ the quantity $\delta(P)^{q-1} = x^{q-1}$ differs from $\prod_{x \in P \setminus \{0\}} x = \prod_{\lambda \in \mathbb{F}_q^\times} (\lambda x) = -x^{q-1}$

³¹Whether such sets \mathcal{N}'_1 are maximal in general remains an open problem.

just by its sign. Hence we have $\delta(W)^{q-1} = (-1)^{q^2+q+1} \prod_{w \in W \setminus \{0\}} w = (-1)^{q^2+q+1} = -1$ as claimed.³²

This gives $\delta(aW) = \mathbb{F}_q a^{q^2+q+1} \epsilon$ and $\delta(aW)^{q-1} = -a^{q^3-1}$ for any $a \in \mathbb{F}_{q^4}^\times$.

Since $\sigma(aW)^{q-1} = \delta(aW)^{q-1} / \delta(Z)^{q^2-1}$, where $Z = W \cap aW$, we also need to compute $\delta(W \cap aW)$. This can be done as follows:

The \mathbb{F}_q -space $W \cap aW$ is the set of zeros of the polynomial

$$\begin{aligned} X^{q^3} + X^{q^2} + X^q + X - a^{q^3} \left((a^{-1}X)^{q^3} - (a^{-1}X)^{q^2} - (a^{-1}X)^q - a^{-1}X \right) \\ = (1 - a^{q^3-q^2})X^{q^2} + (1 - a^{q^3-q})X^q + (1 - a^{q^3-1})X \\ = (1 - a^{q^3-q^2}) \left(X^{q^2} + \frac{1 - a^{q^3-q}}{1 - a^{q^3-q^2}} X^q + \frac{1 - a^{q^3-1}}{1 - a^{q^3-q^2}} X \right), \end{aligned}$$

and hence

$$\begin{aligned} \delta(W \cap aW)^{q-1} &= \frac{1 - a^{q^3-1}}{1 - a^{q^3-q^2}}, \\ \sigma(aW)^{q-1} &= \frac{-a^{q^3-1}(1 - a^{q^3-q^2})^{q+1}}{(1 - a^{q^3-1})^{q+1}} \\ &= -\frac{a^{q^3-1}(1 - a^{1-q^3})(1 - a^{q^3-q^2})}{(1 - a^{1-q})(1 - a^{q^3-1})} \\ &= \frac{1 - a^{q^3-q^2}}{1 - a^{1-q}} = \frac{a^{q-1} - a^{q^3-q^2+q-1}}{a^{q-1} - 1} \\ &= 1 - \frac{a^{q^3-q^2+q-1} - 1}{a^{q-1} - 1} \\ &= 1 - \frac{a^{(q-1)(q^2+1)} - 1}{a^{q-1} - 1}, \end{aligned}$$

as asserted. \square

From Lemma 7 it is clear that $\sigma(E) = \mathbb{F}_q$ for the planes of the form $E = a^{q+1}W \neq W$ and no other planes. Since there are q^2 such planes, we have that $\#\text{Im}(\sigma) \leq q^3 + q^2 + q - (q^2 - 1) = q^3 + q + 1$. It turns out that equality holds in this bound, and hence a maximum of $\#\mathcal{N}'_1 = (q-1)(q^3 + q + 1)$ planes passing through any given point $P \in S$ can be added to \mathcal{L}_0 without increasing t . Before proving this theorem, we note that the existence of collisions already implies that a q -analogue of the Fano plane cannot be constructed by our present method.

Theorem 3. *Let \mathcal{L}_0 be the plane subspace code of size $q^8 - q^7 + q^3$ obtained from the lifted Gabidulin code \mathcal{L} by removing all planes Γ_f corresponding to binomials $f(x) = r(ux^q - u^q x)$ with $r \in \mathbb{F}_{q^4}^\times$, $u \in$*

³²Note that the last equality is trivially true for even q .

$\mathbb{F}_{q^4} \setminus W$. Then \mathcal{L}_0 can be augmented by $(q^4 - 1)(q^3 + q + 1)$ new planes meeting S in a point, $(q - 1)(q^3 + q + 1)$ of them passing through any point $P \in S$, to a subspace code \mathcal{C} with size $\#\mathcal{C} = q^8 + q^5 + q^4 - q - 1$. Moreover, \mathcal{C} may be chosen as a Σ -invariant code.

Proof. As discussed above, we need only show that the values of σ on the $q^3 + q$ planes not of the form $a^{q+1}W$ are distinct. This is equivalent to

$$\frac{x-1}{y-1} \neq \frac{x^{q^2+1}-1}{y^{q^2+1}-1} \quad (6)$$

for any pair of distinct elements $x, y \in \mathbb{F}_{q^4}^\times$ that are $(q-1)$ -th powers but not (q^2+1) -th roots of unity.

Assume by contradiction that equality holds in (6) for some pair x, y . Then, since the right-hand side is in the subfield \mathbb{F}_{q^2} , we can conclude that also

$$\frac{x-1}{y-1} = \left(\frac{x-1}{y-1} \right)^{q^2} = \frac{x^{q^2}-1}{y^{q^2}-1}.$$

The two equations can be rewritten as

$$\begin{aligned} \sum_{i=0}^{q^2} x^i &= \frac{x^{q^2+1}-1}{x-1} = \frac{y^{q^2+1}-1}{y-1} = \sum_{i=0}^{q^2} y^i, \\ \sum_{i=0}^{q^2-1} x^i &= \frac{x^{q^2}-1}{x-1} = \frac{y^{q^2}-1}{y-1} = \sum_{i=0}^{q^2-1} y^i, \end{aligned}$$

and together imply $x^{q^2} = y^{q^2}$ and hence $x = y$; contradiction. \square

Remark 2. The map $\mathbb{F}_q a \mapsto \sigma(aW)$ leaves each coset of the subgroup consisting of the $(q+1)$ -th powers (or (q^2+1) -th roots of unity) in $\mathbb{F}_{q^4}^\times/\mathbb{F}_q^\times$ invariant and induces bijections on all nontrivial cosets; in particular, the set of values excluded from $\text{Im}(\sigma)$ consists of the q^2 points $\neq \mathbb{F}_q$ in $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ that are of the form $\mathbb{F}_q a^{q+1}$.

This refinement of Theorem 3 follows from

$$\begin{aligned} \sigma(aW)^{(q-1)(q^2+1)} &= \left(\frac{a^{q-1} - a^{(q-1)(q^2+1)}}{a^{q-1} - 1} \right)^{q^2+1} = \left(\frac{a^{q-1}(1 - a^{q^3-q^2})}{a^{q-1} - 1} \right)^{q^2+1} \\ &= \left(\frac{a^{q^3-q^2}(1 - a^{q-1})}{a^{q^3-q^2} - 1} \right) \left(\frac{a^{q-1}(1 - a^{q^3-q^2})}{a^{q-1} - 1} \right) \\ &= a^{q^3-q^2+q-1} = a^{(q-1)(q^2+1)}, \end{aligned}$$

which shows the claimed coset invariance, and the known behaviour of $\mathbb{F}_q a \mapsto \sigma(aW)$ on the subgroup of $(q+1)$ -th powers and its complement. In the next section we will discuss the geometric significance of this subgroup.

6. EXTENSIONS

The subspace code \mathcal{C} of Theorem 3 is far from being unique—we can select the $q - 1$ new planes in one of the q^2 “collision classes” independently at each point of S and even mix planes from different collision classes for $q > 2$, resulting in at least $(q^2)^{q^3+q^2+q+1}$ different choices for \mathcal{C} (exactly 4^{15} different choices for $q = 2$).

On the other hand, if we omit the selection of a collision class at every point of S then no ambiguity is introduced. The resulting subspace code, we call it \mathcal{C}_0 , has size $\#\mathcal{C}_0 = \#\mathcal{C} - (q^4 - 1) = q^8 + q^5 - q$ and is clearly Σ -invariant. Moreover, the size of a maximal³³ extension $\overline{\mathcal{C}}_0$ of \mathcal{C}_0 is no less than the size of a maximal extension $\overline{\mathcal{C}}$ of \mathcal{C} .

The planes we should consider for augmenting \mathcal{C}_0 are essentially of two types—at most $q^4 - 1$ planes meeting S in a point and at most $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = q^4 + q^3 + 2q^2 + q + 1$ planes meeting S in a line.³⁴ Hence the size of $\overline{\mathcal{C}}_0$ is a priori bounded by $q^8 + q^5 + q^4 - q - 1 \leq \#\overline{\mathcal{C}}_0 \leq q^8 + q^5 + 2q^4 + q^3 + 2q^2$. For large q one may consider this as a satisfactory answer to the extension problem for \mathcal{C}_0 , but for small values of q this is certainly not true.

For more precise results we need to describe the free lines of \mathcal{C}_0 meeting S in a point. Prior to this description, we collect a few geometric facts about the coset partition of $\mathbb{F}_{q^4}^\times$ relative to the subgroup O of $(q + 1)$ -th powers, and we prove two further auxiliary results, which seem to be of independent interest.

The point set $\mathcal{O} = \{\mathbb{F}_q a^{q+1}; a \in \mathbb{F}_{q^4}^\times\} = \{\mathbb{F}_q x; x \in \mathbb{F}_{q^4}^\times, x^{(q-1)(q^2+1)} = 1\}$ corresponding to O defines an elliptic quadric and hence an ovoid in $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q) \cong \text{PG}(3, \mathbb{F}_q)$. This can be seen by rewriting $x^{(q-1)(q^2+1)} = x^{q^3-q^2+q-1} = 1$ as $x^{q^3+q} - x^{q^2+1} = 0$ and further as $\epsilon x^{q^3+q} - \epsilon x^{q^2+1} = 0$, where $\epsilon^{q-1} = -1$. The map $x \mapsto \epsilon x^{q^3+q} - \epsilon x^{q^2+1}$ takes values in \mathbb{F}_q and hence constitutes a quadratic form on $\mathbb{F}_{q^4}/\mathbb{F}_q$. Since $\#\mathcal{O} = q^2 + 1$, the corresponding quadric must be elliptic.

Hence the coset partition with respect to O determines a partition \mathcal{O} of the point set of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ into $q + 1$ ovoids, which are transitively permuted by $\mathbb{F}_{q^4}^\times$ (acting as a Singer group).³⁵

It is well-known (see e.g. [20], [3] or [9]) that \mathcal{O} has a unique tangent plane in each of its points and meets the remaining $q^3 + q$ planes of $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ in $q + 1$ points (the points of a non-generate conic). The tangent plane to \mathcal{O} in $\mathbb{F}_q = \mathbb{F}_q 1$ is $W' = \epsilon W$ (the plane with equation $\text{Tr}(\epsilon x) = 0$), where as before $\epsilon^{q-1} = -1$. This follows from $\text{Tr}(\epsilon \cdot 1) =$

³³“Maximal” refers to “maximal size”, not the weaker “maximal with respect to set inclusion”.

³⁴Adding planes contained in S to \mathcal{C}_0 is not an option.

³⁵A partition of $\text{PG}(3, \mathbb{F}_q)$ into $q + 1$ ovoids is often called an *ovoidal fibration*. The ovoidal fibration \mathcal{O} has been further investigated in [11].

$\text{Tr}(\epsilon) = \epsilon - \epsilon + \epsilon - \epsilon = 0$ and

$$\begin{aligned} \text{Tr}(\epsilon a^{q+1}) &= \epsilon a^{q+1} - \epsilon a^{q^2+q} + \epsilon a^{q^3+q^2} - \epsilon a^{1+q^3} \\ &= \epsilon(a - a^{q^2})(a^q - a^{q^3}) = \epsilon(a - a^{q^2})^{q+1}, \end{aligned}$$

which shows that $\mathbb{F}_q a^{q+1} \notin \epsilon W$ unless $\mathbb{F}_q a^{q+1} = \mathbb{F}_q$.

It follows that each plane E is tangent to a unique ovoid in \mathcal{O} and meets the remaining q ovoids in $q+1$ points. More precisely, $E = aW$ is tangent to $a\mathcal{O}$ in $a\epsilon$, as follows from $\epsilon\mathcal{O} = \mathcal{O}$.³⁶

In particular, W itself is tangent to \mathcal{O} in $\mathbb{F}_q\epsilon$, and the points of W are partitioned into the singleton $\{\mathbb{F}_q\epsilon\}$ and q ovoid sections $W \cap \alpha^i\mathcal{O}$, $1 \leq i \leq q$, of size $q+1$.

Now recall from Section 5 that $L \mapsto \delta(L)$ maps the pencil of all lines through $\mathbb{F}_q a$ bijectively onto the plane $a^{q+1}W$. The planes of this form are exactly the tangent planes to \mathcal{O} and represent a dual ovoid \mathcal{O}^* in $\text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$. Hence we can dualize each of the above properties. In particular this gives that the q^2 planes in $\mathcal{O}^* \setminus \{W\}$ (i.e. those with $\sigma(E) = \mathbb{F}_q$, the “colliding planes”) intersect W in the q^2 lines not passing through the distinguished point $\mathbb{F}_q\epsilon$.³⁷

Our final and most important geometric observation relates the line orbits of the Singer group $\mathbb{F}_{q^4}^\times$ to the ovoidal fibration \mathcal{O} . Since $\delta(rL) = r^{q+1}\delta(L)$ for $r \in \mathbb{F}_{q^4}^\times$, every line orbit $[L]$ corresponds to a unique ovoid in \mathcal{O} (the ovoid containing the point $\delta(L)$). The map $[L] \rightarrow \delta(L)\mathcal{O}$ must be a bijection, since this is true for $L \mapsto \delta(L)$ at any fixed point $\mathbb{F}_q a$ and every line orbit (resp., ovoid) contains a line through $\mathbb{F}_q a$ (resp., has a nonempty ovoid section in $a^{q+1}W$).

In fact the foregoing shows that there are q regular line orbits $[L]$ (i.e., of length $q^3 + q^2 + q + 1$) and one “short” line orbit of length $q^2 + 1$ represented by the subfield \mathbb{F}_{q^2} (since $\delta(\mathbb{F}_{q^2}) = \mathbb{F}_q\epsilon$). The short orbit contains exactly one line through each point (i.e., it forms a line spread); any regular orbit contains $q+1$ lines through each point $\mathbb{F}_q a$, which form a quadric cone with vertex $\mathbb{F}_q a$; in particular no three of these $q+1$ lines are coplanar.³⁸

We have seen in Lemma 5 that $a, b \in W$ implies $\epsilon\delta(a, b) \in W$ (i.e. $\delta(Z) \in W' = \epsilon W$ for any line $Z = \langle a, b \rangle \subset W$). The following similar but less obvious result will be used in the sequel.

Lemma 8. *For $a, b \in W$ we also have $\epsilon a^{q^3}\delta(a, b)^{q+1} \in W$.*

This is easily seen to be equivalent to $z^{q^3}\delta(Z)^{q+1} \in W'$ for all lines Z in W and all points $\mathbb{F}_q z$ on Z .

³⁶Note that $\mathbb{F}_q\epsilon \in \mathcal{O}$. For even q this is trivial. If q is odd and α is a primitive element of \mathbb{F}_{q^4} then $\epsilon = \alpha^{(q^3+q^2+q+1)/2} = (\alpha^{(q^2+1)/2})^{q+1}$ satisfies $\epsilon^{q-1} = -1$ and is a $(q+1)$ -th power in $\mathbb{F}_{q^4}^\times$.

³⁷The point $\mathbb{F}_q\epsilon$ represents the dual tangent plane to \mathcal{O}^* in W , and the q^2 lines represent the dual lines connecting $W \in \mathcal{O}^*$ to the remaining points of \mathcal{O}^* .

³⁸See [19] for more information on this.

Proof. First note that W contains a unique line $L_0 = \mathbb{F}_{q^2}\varepsilon$ of the short line orbit, which is determined by $\varepsilon^{q^2-1} = -1$.³⁹ Since the map $W \rightarrow \mathbb{F}_{q^4}$, $b \mapsto \varepsilon a^{q^3} \delta(a, b)^{q+1}$ is constant on lines through $\mathbb{F}_q a$, it suffices to consider the cases (i) $\mathbb{F}_q a \notin L_0$, $\mathbb{F}_q b \in L_0$ and (ii) $\mathbb{F}_q a \in L_0$, $b \in W$ arbitrary.

(i) Since all nonzero elements $b \in L_0$ satisfy $b^{q^2-1} = -1$, we write $b = \varepsilon$ in this case. Our task is to show that the alternating sum of the conjugates (over \mathbb{F}_q) of

$$\begin{aligned} a^{q^3} \delta(a, \varepsilon)^{q+1} &= a^{q^3} (a\varepsilon^q - a^q\varepsilon)(a^q\varepsilon^{q^2} - a^{q^2}\varepsilon^q) = -a^{q^3} (a\varepsilon^q - a^q\varepsilon)(a^q\varepsilon + a^{q^2}\varepsilon^q) \\ &= -a^{q^3+q+1}\varepsilon^{q+1} + a^{q^3+2q}\varepsilon^2 - a^{q^3+q^2+1}\varepsilon^{2q} + a^{q^3+q^2+q}\varepsilon^{q+1} \end{aligned}$$

is equal to zero. Since a^{q^3+q+1} and $a^{q^3+q^2+q}$ are conjugate and $\varepsilon^{q+1} = \varepsilon$, the alternating sums of the conjugates of the first and last summand cancel. For the two summands in the middle we obtain likewise

$$\begin{aligned} &a^{q^3+2q}\varepsilon^2 - a^{2q^2+1}\varepsilon^{2q} + a^{2q^3+q}\varepsilon^2 - a^{q^2+2}\varepsilon^{2q} \\ &\quad - (a^{q^3+q^2+1}\varepsilon^{2q} - a^{q^3+q+1}\varepsilon^2 + a^{q^2+q+1}\varepsilon^{2q} - a^{q^3+q^2+q}\varepsilon^2) \\ &= a^{q^3+q}(a^q + a^{q^3} + a + a^{q^2})\varepsilon^2 - a^{q^2+1}(a^{q^2} + a + a^{q^3} + a^q)\varepsilon^{2q} = 0, \end{aligned}$$

since $a \in W$.

(ii) Writing $a = \varepsilon$, we have

$$\begin{aligned} \varepsilon^{q^3} \delta(\varepsilon, b)^{q+1} &= -\varepsilon^q (\varepsilon b^q - \varepsilon^q b)(\varepsilon^q b^{q^2} + \varepsilon b^q) \\ &= b^{q+1}\varepsilon^{2q+1} - b^{2q}\varepsilon^{q+2} + b^{q^2+1}\varepsilon^{3q} - b^{q^2+q}\varepsilon^{2q+1}. \end{aligned}$$

The alternating sum of the conjugates of the third summand is $b^{q^2+1}\varepsilon^{3q} + b^{q^3+q}\varepsilon^3 - b^{q^2+1}\varepsilon^{3q} - b^{q^3+q}\varepsilon^3 = 0$. For the alternating sum of the conjugates of the rest we obtain, using $(\varepsilon^{2q+1})^q = \varepsilon^{2q^2+q} = \varepsilon^{q+2}$, $(\varepsilon^{q+2})^q = \varepsilon^{q^2+2q} = -\varepsilon^{2q+1}$ and $b^{q+1} + b^2 + b^{q^3+1} = (b^q + b + b^{q^3})b = -b^{q^2+1}$, etc.,

$$\begin{aligned} &(b^{q+1} - b^{q^3+q^2} - b^{2q^2} + b^2 - b^{q^2+q} + b^{q^3+1})\varepsilon^{2q+1} \\ &\quad + (-b^{q^2+q} + b^{q^3+1} - b^{2q} + b^{2q^3} + b^{q^3+q^2} - b^{q+1})\varepsilon^{q+2} \\ &= (-b^{q^2+1} + b^{q^2+1})\varepsilon^{2q+1} + (b^{q^3+q} - b^{q^3+q})\varepsilon^{q+2} = 0. \end{aligned}$$

This completes the proof of the lemma. \square

The second auxiliary result is the projective version of Lemma 7.

Lemma 9. *For $a \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ we have $\sigma(aW) = \mathbb{F}_q \varepsilon a^{-q}(a^q - a)^{q+1}$.⁴⁰*

³⁹Thus L_0 is the \mathbb{F}_{q^2} -analogue of the point $\mathbb{F}_q \varepsilon$ and can also be seen as the kernel of the relative trace map $\text{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_{q^2}}$.

⁴⁰Note that $aW = W$ is equivalent to $a \in \mathbb{F}_q^\times$ (e.g., by Singer's Theorem).

Proof. By Lemma 7,

$$\begin{aligned}\sigma(aW)^{q-1} &= \frac{a^{q-1} - a^{q^3-q^2+q-1}}{a^{q-1} - 1} = \frac{a^q - a^{q^3-q^2+q}}{a^q - a} = -\frac{a^{q^3} - a^{q^2}}{a^{q^2-q}(a^q - a)} \\ &= -\frac{(a^q - a)^{q^2-1}}{a^{q^2-q}} = \left(\epsilon \cdot \frac{(a^q - a)^{q+1}}{a^q} \right)^{q-1}.\end{aligned}$$

The result follows. \square

Now we are ready to resume the analysis of augmenting \mathcal{C}_0 . Recall from Section 5 that the $(q-1)(q^3+q)$ planes in \mathcal{C}_0 meeting S in $P_1 = \mathbb{F}_q(0, 1)$ have the form $N = N(Z, P_1, g) = \{(x, g(x)+\nu); x \in Z, \nu \in \mathbb{F}_q\}$, where $Z = \langle a, b \rangle \subset W$ is 2-dimensional, $g(x) = \delta(\lambda d + \mu c, x)/\delta(a, b)$ and the plane $E = \langle a, b, \lambda d + \mu c \rangle$ is not of the form $u^{q+1}W$.

In what follows, by a *free line* we mean a line not covered by a plane in \mathcal{C}_0 , and by a *free plane* a plane which contains only free lines and hence can be individually added to \mathcal{C}_0 without increasing t . From Section 5 we know that the $(q-1)q^2$ planes $N(Z, P_1, g)$ with E of the form $u^{q+1}W$ and their images under Σ are free. We will denote this set of $(q^4-1)q^2$ free planes by \mathcal{N}'' , so that $\mathcal{N} = \mathcal{N}' \uplus \mathcal{N}''$ in the terminology of Section 5.

For the statement of the next lemma recall that the 4-flats in $\text{PG}(W \times \mathbb{F}_{q^4})$ above S are of the form $F = \mathbb{F}_q x \times \mathbb{F}_{q^4} = \mathbb{F}_q(x, 0) + S$ with $\mathbb{F}_q x$ a point in W (i.e. $x \in W$ is uniquely determined up to scalar multiples in \mathbb{F}_q^\times).

Lemma 10. *Let $F = \mathbb{F}_q x \times \mathbb{F}_{q^4}$ be a 4-flat containing S and $P_0 = \mathbb{F}_q(x, 0) = F \cap W$.*

- (i) *A line $L \subset F$ meeting S in a point is free if and only if either $P_0 \in L$ or the plane generated by P_0 and L meets S in a line L' such that $\delta(L') \in x^q \mathcal{O}$.*
- (ii) *A plane $E \subset F$ meeting S in a line L' is free if and only if $P_0 \in E$ and $\delta(L') \in x^q \mathcal{O}$.*

Note that, in view of the preceding discussion, the condition $\delta(L') \in x^q \mathcal{O}$ holds precisely for the lines L' in a certain line orbit of $\mathbb{F}_{q^4}^\times$ on $\text{PG}(S/\mathbb{F}_q) \cong \text{PG}(\mathbb{F}_{q^4}/\mathbb{F}_q)$. Points $\mathbb{F}_q x, \mathbb{F}_q x'$ in the same ovoid section $W \cap x\mathcal{O} = W \cap x'\mathcal{O}$ are associated with the same line orbit, and the induced map from ovoid sections to line orbits is a bijection.⁴¹ Moreover, the degenerate ovoid section $\{\mathbb{F}_q \epsilon\}$ is associated with the short line orbit $[\mathbb{F}_{q^2}]$ (since $\delta(\mathbb{F}_{q^2}) = \mathbb{F}_q \epsilon \in \mathcal{O} = \epsilon^q \mathcal{O}$).

⁴¹The ovoid $x^q \mathcal{O} = (x\mathcal{O})^q$ differs from $x\mathcal{O}$ only by conjugation with the Frobenius automorphism of $\mathbb{F}_{q^4}/\mathbb{F}_q$. If we choose orbit representatives with $1 \in L'$ then the condition of the lemma becomes $\delta(L') \in W \cap x^q \mathcal{O}$, the conjugate ovoid section in W .

Proof of the lemma. Since the sets of free lines and free planes, as well as the stated conditions, are Σ -invariant, it suffices to consider the cases $P_1 \in L$ and $P_1 \in E$.

(i) The line $L_0 = \langle P_0, P_1 \rangle = \mathbb{F}_q x \times \mathbb{F}_q$ is free, since $N = N(Z, P_1, g) \in \mathcal{C}_0$ has $g(x) = \delta(\lambda d + \mu c, x)/\delta(a, x) \notin \mathbb{F}_q$. The remaining $q^3 - 1$ lines in F meeting S in P_1 have the form $L = \mathbb{F}_q(x, y) + P_1$ with $y \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ and correspond to nontrivial additive cosets of \mathbb{F}_q in \mathbb{F}_{q^4} . Inspecting the proof of Lemma 6 shows that such a line L is free iff $\mathbb{F}_q(y^q - y) = \mathbb{F}_q\delta(1, y) \neq x^q\sigma(E)$ for all planes E through $\mathbb{F}_q x$ with $E \notin \mathcal{O}^*$. Since this condition depends only on $\mathbb{F}_q^\times y$, the free lines form a union of planes through L_0 whose intersecting lines $L' = \langle 1, y \rangle$ with S are determined by the conditions $\delta(L') \neq x^q\sigma(E)$.⁴²

The planes $E = uW$ containing $\mathbb{F}_q x$ are characterized by $x/u \in W$. One such plane is W , which will be excluded from now on. Using Lemma 9, homogeneity of δ and Lagrange's Theorem for the group $\mathbb{F}_{q^4}^\times/\mathbb{F}_q$, we obtain

$$\begin{aligned} x^q\sigma(uW) &= \mathbb{F}_q\epsilon(x/u)^q\delta(1, u)^{q+1} = \mathbb{F}_q\epsilon(u/x)^{q^2+q+1}\delta(x/u, x)^{q+1} \\ &= \mathbb{F}_q\epsilon(x/u)^{q^3}\delta(x/u, x)^{q+1}. \end{aligned}$$

By Lemma 8, $x^q\sigma(uW) \in W$ for all planes $uW \neq W$ containing $\mathbb{F}_q x$. Now we distinguish two cases.

Case 1: $\mathbb{F}_q x = \mathbb{F}_q \epsilon$. In this case, since no plane in \mathcal{O}^* except W passes through $\mathbb{F}_q \epsilon$, all $q^2 + q$ planes $uW \neq W$ containing $\mathbb{F}_q \epsilon$ provide a condition $\delta(L') \neq \epsilon^q\sigma(uW)$. But $\delta(L') \in W$ and the invariants $\sigma(uW)$ are distinct and $\neq 1$. Hence $\delta(L') = \mathbb{F}_q \epsilon^q = \mathbb{F}_q \epsilon$ remains as the only possibility. This implies $L' = \mathbb{F}_{q^2}$ and $\delta(L') \in \epsilon\mathcal{O} = \mathcal{O}$ as asserted.

Case 2: $\mathbb{F}_q x \neq \mathbb{F}_q \epsilon$. In this case exactly q of the planes in \mathcal{O}^* pass through $\mathbb{F}_q x$ and the condition $\delta(L') \neq x^q\sigma(uW)$ applies to q^2 planes. Since $(x/u)^{q^3} \in x^{q^3}\mathcal{O}$ iff $u^{q^3} \in \mathcal{O}$ iff $u \in \mathcal{O}$, we must have $x^q\sigma(uW) \notin x^{q^3}\mathcal{O}$ for these q^2 planes. Hence the q^2 values taken by $x^q\sigma(uW)$ form the complementary set $W \setminus x^{q^3}\mathcal{O}$ and the condition reduces to $\delta(L') \in x^{q^3}\mathcal{O}$. Since $x^{q^3-q} = (x^{q^2-q})^{q+1} \in \mathcal{O}$, this is in turn equivalent to $\delta(L') \in x^q\mathcal{O}$ as asserted.

(ii) Clearly any plane satisfying these conditions is free. Conversely, if E is free and $P_0 \in E$ then Part (i) can be applied to any line $L \subset E$ satisfying $P_0 \notin L \neq L'$ and gives $\delta(L') \in x^q\mathcal{O}$. Thus it remains to show that in the case $P_0 \notin E$ the plane E cannot be free.

Consider the solid $T = \langle E, P_0 \rangle$, which meets S in a plane $E' \supset L'$. Connecting P_0 to the $q^2 + q$ lines $\neq L'$ in E and applying Part (i) gives that all lines $\neq L'$ in E' must be in the same line orbit of $\mathbb{F}_{q^4}^\times$ in

⁴²The points in $\langle L_0, L' \rangle$ on the $q - 1$ lines through P_1 different from L_0, L' are those of the form $\mathbb{F}_q(x, y')$ with y' in the $\text{AGL}(1, \mathbb{F}_q)$ -orbit $\mathbb{F}_q^\times y + \mathbb{F}_q$.

$\text{PG}(S/\mathbb{F}_q)$. Since E' contains no more than $q+1$ lines of any line orbit,⁴³ we have a contradiction, and the proof of the lemma is complete. \square

In the sequel we write \mathcal{E} for the set of free planes meeting S in a line. Part (ii) of Lemma 10 says that the planes in \mathcal{E} have the form $\mathbb{F}_q x \times L'$ (“decomposable” planes) with L' in the line orbit associated to $\mathbb{F}_q x$.

Clearly the largest extension (still having $t = 2$) of \mathcal{C}_0 by planes in \mathcal{E} is obtained in the following way: (i) Add all $q^2 + 1$ planes generated by $\mathbb{F}_q(\epsilon, 0)$ and a line in the short line orbit of $\mathbb{F}_{q^4}^\times$ on $\text{PG}(S/\mathbb{F}_q)$. These planes have the form $\mathbb{F}_q \epsilon \times (\mathbb{F}_{q^2})r$ with $r \in \mathbb{F}_{q^4}^\times / \mathbb{F}_{q^2}^\times$. (ii) For each ovoid section $W \cap x\mathcal{O}$ of size $q+1$ decompose the associated regular line orbit $[L']$ of $\mathbb{F}_{q^4}^\times$ on $\text{PG}(S/\mathbb{F}_q)$ into $q+1$ mutually disjoint partial spreads and a remainder of minimum size (i.e., the union of the partial spreads, a subset of $[L']$, should have maximum size). Choose a bijection from $W \cap x\mathcal{O}$ to the set of these partial spreads and add all planes $\mathbb{F}_q x' \times L$ with $\mathbb{F}_q x' \in W \cap x\mathcal{O}$ and L a line in the partial spread corresponding to $\mathbb{F}_q x'$.

For small values of q it turns out that the regular Singer line orbits of $\text{PG}(3, \mathbb{F}_q)$ admit decompositions into fairly large partial spreads. As a consequence, maximal extensions of \mathcal{C}_0 by planes in \mathcal{E} improve on the code \mathcal{C} of Theorem 3. Below we will discuss in more detail the cases $q = 2, 3$, where the number of additional planes is 29 and 114 respectively.⁴⁴

Of course we are ultimately interested in finding the largest extension of \mathcal{C}_0 by planes of any of the two types. For $q = 2$ it turns out that all but one of the theoretical maximum of $15 + 29 = 44$ additional planes can be added to \mathcal{C}_0 , resulting in the largest presently known subspace code $\overline{\mathcal{C}}_0$ of size $286 + 43 = 329$; cf. [5, 27]. This case will be considered further below, culminating in a computer-free construction of one such code.

It seems difficult, however, to generalize the analysis in the binary case to larger values of q . In the ternary case $q = 3$ the largest extension of \mathcal{C}_0 we have found by a computer search has size $\#\overline{\mathcal{C}}_0 = 6977$,⁴⁵ but we do not yet know whether this is the true maximum.

We summarize our present knowledge about the extension problem for \mathcal{C}_0 in the following theorem. Part (i) and (ii) are the result of a computer search. For the computation of canonical forms and automorphism groups of subspace codes, the algorithm in [16] (based

⁴³More precisely, the lines in E' fall into $q+1$ orbits—a single line in the short orbit and $q+1$ lines forming a dual conic in each of the q regular orbits.

⁴⁴Compare this with the number $q^4 - 1 = 15$ resp. 80 of planes in \mathcal{N}'' that can be added to \mathcal{C}_0 , and also with the theoretical maximum of $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = 35$ resp. 130 additional planes in \mathcal{E} .

⁴⁵Compare this with the upper bound $\#\overline{\mathcal{C}}_0 \leq 6801 + 80 + 114 = 6995$.

on [15], see also [17]) is used. Part (iii) represents a slight improvement of Theorem 3 for general q .

Theorem 4. *Let \mathcal{C}_0 be the plane subspace code of size $q^8 + q^5 - q$ obtained by the expurgation-augmentation process described in Section 5 and with no planes in \mathcal{N}'' selected.*

- (i) *For $q = 2$ maximal extensions $\overline{\mathcal{C}_0}$ of \mathcal{C}_0 have size $\#\overline{\mathcal{C}_0} = 329$. There exist 26 496 different isomorphism types of such extensions, all with trivial automorphism group. Moreover, both possible intersection patterns with S , viz. $(a_0, a_1, a_2, a_3) = (136, 164, 29, 0)$ and $(136, 165, 28, 0)$, occur with numbers of isomorphism types 10 368 and 16 128, respectively.*
- (ii) *For $q = 3$ there exists an extension $\overline{\mathcal{C}_0}$ of size $\#\overline{\mathcal{C}_0} = 6977$.*
- (iii) *For general q there exists an extension $\overline{\mathcal{C}_0}$ of size $\#\overline{\mathcal{C}_0} = q^8 + q^5 + q^4 + q^2 - q$, obtained by adding to the subspace code \mathcal{C} of Theorem 3 the $q^2 + 1$ planes in \mathcal{E} of the form $\mathbb{F}_q\epsilon \times (\mathbb{F}_{q^2})r$, $r \in \mathbb{F}_{q^4}^\times / \mathbb{F}_{q^2}^\times$.*

Proof of Part (iii). Since W is the tangent plane to \mathcal{O} in $\mathbb{F}_q\epsilon$, W meets the remaining q^2 tangent planes in \mathcal{O}^* in the q^2 lines not passing through $\mathbb{F}_q\epsilon$. This means that the planes in \mathcal{N}'' have the form $N(Z, P, g)$ with Z not passing through $\mathbb{F}_q\epsilon$ and hence do not interfere with the $q^2 + 1$ new planes, which have the form $E = E(\mathbb{F}_q\epsilon, (\mathbb{F}_{q^2})r, 0)$.⁴⁶ \square

In the remainder of this section we will present a computer-free construction of a maximal extension $\overline{\mathcal{C}_0}$ in the case $q = 2$ and briefly comment on the case $q = 3$, which is remarkable in several respects.⁴⁷

Representing \mathbb{F}_{16} as $\mathbb{F}_2[\alpha]$ with $\alpha^4 + \alpha + 1 = 0$, we have $\mathbb{F}_{16}^\times = \langle \alpha \rangle$ and $W = \{1, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^8, \alpha^{10}\}$.⁴⁸ The subfield $\mathbb{F}_4 \subset \mathbb{F}_{16}$ represents a line of $\text{PG}(3, \mathbb{F}_2)$ and generates the short line orbit $[\mathbb{F}_4] = \{\mathbb{F}_4\alpha^{3i}; 0 \leq i \leq 4\}$. In addition there are two regular line orbits represented by $L_1 = \{1, \alpha, \alpha^4\}$ and $L_2 = \{1, \alpha^2, \alpha^8\} = \varphi(L_1)$. The remaining lines through 1 are $\{1, \alpha^3, \alpha^{14}\}$, $\{1, \alpha^{11}, \alpha^{12}\}$ in $[L_1]$ and $\{1, \alpha^6, \alpha^{13}\}$, $\{1, \alpha^7, \alpha^9\}$ in $[L_2]$. The ovoidal fibration is $\mathcal{O} = \{\mathcal{O}, \alpha\mathcal{O}, \alpha^2\mathcal{O}\}$ with $\mathcal{O} = \{\alpha^{3i}; 0 \leq i \leq 4\}$, and the corresponding W -sections are $\mathcal{O} \cap W = \{1\}$, $\alpha\mathcal{O} \cap W = \{\alpha, \alpha^4, \alpha^{10}\}$, $\alpha^2\mathcal{O} \cap W = \{\alpha^2, \alpha^5, \alpha^8\}$.

Decomposing $[L_1]$, $[L_2]$ into partial spreads is best done in a graph-theoretic setting. We view the lines in each orbit as vertices of a circulant graph via $\alpha^i L \mapsto i \in \mathbb{Z}_{15}$. Then $\alpha^i L \cap \alpha^j L \neq \emptyset$ iff $j - i \in \{\pm 1, \pm 3, \pm 4\}$ for $L \in [L_1]$, and similarly for $[L_2]$.⁴⁹ In this way partial

⁴⁶Viewed geometrically, the planes in \mathcal{N}'' contain no points in $(\mathbb{F}_q\epsilon \times \mathbb{F}_{16}) \setminus S$ and hence cannot have a line with a plane $\mathbb{F}_q\epsilon \times (\mathbb{F}_{q^2})r$ in common.

⁴⁷Verehrter Jubilar, Sie haben sicher schon bemerkt, dass die Ordnung der multiplikativen Gruppe \mathbb{F}_{34}^\times gerade 80 ist.

⁴⁸We can represent the points of $\text{PG}(3, \mathbb{F}_2)$ by the nonzero elements of \mathbb{F}_{16}^\times .

⁴⁹In general the circulant graph associated with a regular line orbit has as its connection set the pairwise differences of the logs in $\mathbb{F}_{q^4}^\times / \mathbb{F}_q^\times$ of the points on a representative line.

spreads in the line orbits correspond to cocliques (independent sets) of the associated circulant graph, and an optimal decomposition into $q+1 = 3$ partial spreads corresponds to a 3-colorable (vertex) subgraph of maximum size. In the case under consideration the two graphs are isomorphic (since the orbits are interchanged by φ) and have chromatic number 4. It is readily seen that the maximum cocliques in Γ_1 (the graph corresponding to $[L_1]$) are $S = \{0, 2, 7, 9\}$ and its cyclic shifts modulo 15, and that $\{S, S+1, S+4\}$ forms an optimal decomposition of $[L_1]$ into 3 partial spreads of size 4 (and some remainder of size 3).

At this point we see that \mathcal{C}_0 can be extended by $29 = 5 + 4 + 4 + 4 + 4 + 4 + 4$ planes meeting S in a line. In what follows, we choose the corresponding partial line spreads as the short line orbit (a total spread) for $F = \mathbb{F}_2 \times \mathbb{F}_{16} = \mathbb{F}_2 \times \mathbb{F}_{16}$ and the six partial spreads corresponding to $S, S+1, S+4$ and their images under φ .⁵⁰

We have yet at our disposal the actual “wiring” between the six points $x \in W \setminus \{1\}$ and the six partial line spreads. Since $\delta(L_1) = 1 \cdot \alpha \cdot \alpha^4 = \alpha^5 \in \alpha^2 \mathcal{O}$, Lemma 10 only stipulates that the points in $W \cap \alpha \mathcal{O} = \{\alpha^1, \alpha^4, \alpha^{10}\}$ are connected to the three line spreads in $[L_1]$ and the points in $\{\alpha^2, \alpha^5, \alpha^8\}$ to the three line spreads in $[L_2]$. The actual choice of the bijections (out of six feasible choices for each of the two ovoid sections) should maximize the number of planes in \mathcal{N}'' that can be added to further extend the resulting subspace code of size $286 + 29 = 315$.

In order to solve this problem, we must take a closer look at the lines covered by the planes in \mathcal{N}'' and how these relate to the lines covered by the extended code of size 315. The “local” situation at $P_1 = \mathbb{F}_2(0, 1)$ is depicted in the following table:

$x \backslash L'$	5, 10	1, 4	2, 8	3, 14	6, 13	11, 12	7, 9
0		×	×	×	×	×	×
5	×	×	c	×		×	
10	×	c	×		×		×
1	×		×	c	×		×
2	×	×		×	c	×	
4	×		×		×	c	×
8	×	×		×		×	c

The rows of the table are indexed with the logs of the elements $x \in W$ (corresponding to the 4-flats F above W), the columns with pairs (i, j) such that $\alpha^i + \alpha^j = 1$ (corresponding to the lines L' in $\text{PG}(\mathbb{F}_{16}/\mathbb{F}_2)$ through 1), and the table entries ‘×’, ‘c’ indicate that the plane $\mathbb{F}_2 x \times L'$

⁵⁰This choice is closely related to the essentially unique packing of the 35 lines of $\text{PG}(3, \mathbb{F}_2)$ into 7 spreads, which represents a solution to Kirkman’s Schoolgirl Problem. The packing is obtained by applying a certain cyclic shift modulo 15 to the second orbit decomposition and then adding the 3 lines omitted from each orbit decomposition to the partial spreads in the other set, one at a time.

conflicts with a plane in \mathcal{C}_0 (i.e. $\mathbb{F}_2x \times L' \notin \mathcal{E}$), respectively, with the two planes $N = N(Z, P_1, g) \in \mathcal{N}''$ that have $x \in Z$. For this recall that in general the q planes in \mathcal{N}'' of the form $N(Z, P_1, g)$ with $x \in Z$ cover the same set of $q - 1$ lines meeting S in a point, and that these lines are in the plane $\mathbb{F}_q x \times L'$ with L' determined by $\delta(L') = \mathbb{F}_q x^q$.⁵¹

Now suppose we connect $x \in \{\alpha^1, \alpha^4, \alpha^{10}\}$ to one of the three partial line spreads in $[L_1]$, say \mathcal{S} . Then, writing $P_r = \mathbb{F}_2(0, r)$ and using the action of Σ on \mathcal{N}'' , we see that the planes $N = N(Z, P_r, g) \in \mathcal{N}''$ with $x \in Z$ conflict with $\mathbb{F}_2x \times (rL')$, where L' is the line through 1 matched to x by the 'c' entries in the table. Thus there are precisely 4 values of r for which the later choice of a plane $N = N(Z, P_r, g) \in \mathcal{N}''$ with $x \in Z$ is forbidden, viz. those r for which $rL' \in \mathcal{S}$.⁵² Applying the same reasoning to all $x \in W \setminus \{1\}$ and all valid choices for \mathcal{S} , we obtain the following 3×3 arrays of forbidden values for r . As before, elements of \mathbb{F}_{16}^\times are represented by their logs with respect to α , and in place of the partial spreads we have listed the corresponding cocliques of the circulant graph.⁵³ Further, the ordering of $W \setminus \{1\}$ is chosen in such a way that the arrays are symmetric with respect to the main diagonal.⁵⁴

$x \setminus \mathcal{S}$	0, 2, 7, 9	1, 3, 8, 10	4, 6, 11, 13
10	0, 2, 7, 9	1, 3, 8, 10	4, 6, 11, 13
1	1, 3, 8, 10	2, 4, 9, 11	5, 7, 12, 14
4	4, 6, 11, 13	5, 7, 12, 14	8, 10, 0, 2

$x \setminus \mathcal{S}$	0, 4, 14, 3	2, 6, 1, 5	8, 12, 7, 11
5	0, 4, 14, 3	2, 6, 1, 5	8, 12, 7, 11
2	2, 6, 1, 5	4, 8, 3, 7	10, 14, 9, 13
8	8, 12, 7, 11	10, 14, 9, 13	1, 5, 0, 4

The task is now to match, for each of the two tables, the row labels to the column labels in such a way that the number of points P_r that admit a non-conflicting choice $N = N(Z, P_r, g)$, i.e. a choice of Z such that r is forbidden for no $x \in Z$, is maximized.

A moments reflection shows that the best we can do is to use the main diagonals of the tables (or one of the other two row-and-column transversals without repeated 4-tuples) for the matching, i.e. $10 \mapsto \{0, 2, 7, 9\}$, $1 \mapsto \{1, 3, 8, 10\}$, $4 \mapsto \{4, 6, 11, 13\}$, and similarly for the second table. This ensures that for each P_r at most two points $x_1, x_2 \in W \setminus \{1\}$ are forbidden and leads to a valid choice for Z unless the line through x_1, x_2 contains 1.⁵⁵ Since the only such line is $\{1, \alpha^5, \alpha^{10}\}$ and the three 4-tuples in the first row of the first table are transversal to

⁵¹The planes $E \in \mathcal{O}^* \setminus \{W\}$ parametrizing the planes in \mathcal{N}'' have $\sigma(E) = \mathbb{F}_q$, whence $\delta(L') = \sigma(E)x^q = \mathbb{F}_q x^q$; cf. the proof of Lemma 6.

⁵²Since $L' \in [L_1]$ and $[L_1]$ is regular, the correspondence $r \mapsto rL'$ is a bijection.

⁵³Thus, for example, 0, 2, 7, 9 refers to the partial spread $\mathcal{S} = \{\alpha^0 L_1, \alpha^2 L_1, \alpha^7 L_1, \alpha^9 L_1\}$ with lines $\alpha^0 L_1 = \{1, \alpha, \alpha^4\}$, $\alpha^2 L_1 = \{\alpha^2, \alpha^3, \alpha^6\}$, $\alpha^7 L_1 = \{\alpha^7, \alpha^8, \alpha^{11}\}$, $\alpha^9 L_1 = \{\alpha^9, \alpha^{10}, \alpha^{13}\}$, and 0, 4, 14, 3 to the partial spread $\mathcal{S}' = \{\alpha^0 L_2, \alpha^4 L_2, \alpha^{14} L_2, \alpha^3 L_2\} = \varphi(\mathcal{S})$.

⁵⁴This can be done, since the offsets of the cocliques are the same as that of the lines through 1.

⁵⁵This is the only way to block all four lines $Z \subset W$ (the passants to 1) by a 2-set.

the corresponding 4-tuples of the second table, we can make a non-conflicting choice of Z for all but one P_r . When using the two main diagonals the “bad” point is P_{11} .

In all, we can extend \mathcal{C}_0 by $29 + 14 = 43$ planes to a subspace code $\overline{\mathcal{C}}_0$ of size 329 as claimed.

Finally, we consider briefly the case $q = 3$. Here the number of points and lines in S are 40 and 130, respectively, with line orbit sizes 10, 40, 40, 40. Representing \mathbb{F}_{81} as $\mathbb{F}_3[\alpha]$ with $\alpha^4 - \alpha^3 - 1 = 0$ (a generator of \mathbb{F}_{81}^\times) and the points of $\text{PG}(\mathbb{F}_{81}/\mathbb{F}_3)$ as α^i , $0 \leq i < 40$, we obtain

$$W = \{\alpha^5, \alpha^{13}, \alpha^{15}, \alpha^{20}, \alpha^{22}, \alpha^{25}, \alpha^{26}, \alpha^{31}, \alpha^{34}, \alpha^{35}, \alpha^{37}, \alpha^{38}, \alpha^{39}\}$$

with ovoid sections $W \cap \mathcal{O} = \{\alpha^{20}\}$, $W \cap \alpha\mathcal{O} = \{\alpha^5, \alpha^{13}, \alpha^{25}, \alpha^{37}\}$, $W \cap \alpha^2\mathcal{O} = \{\alpha^{22}, \alpha^{26}, \alpha^{34}, \alpha^{38}\}$, $W \cap \alpha^3\mathcal{O} = \{\alpha^{15}, \alpha^{31}, \alpha^{35}, \alpha^{39}\}$ and corresponding line orbit representatives

$$L_0 = \mathbb{F}_9 = \{\alpha^0, \alpha^{10}, \alpha^{20}, \alpha^{30}\},$$

$$L_1 = \{\alpha^0, \alpha^2, \alpha^{18}, \alpha^{25}\},$$

$$L_2 = \{\alpha^0, \alpha^1, \alpha^{28}, \alpha^{37}\},$$

$$L_3 = \{\alpha^0, \alpha^5, \alpha^{11}, \alpha^{19}\}.$$

The orbit $[L_2]$ is φ -invariant and admits a decomposition into 4 spreads, corresponding to the cocliques $S = \{0, 2, 8, 10, 16, 18, 24, 26, 32, 34\}$, $S + 1$, $S + 4$, $S + 5$.⁵⁶ The other two regular line orbits L_1 , L_3 are interchanged by φ and admit an (optimal) decomposition into 5 partial spreads of size 8. For $[L_1]$ the corresponding cocliques are $T = \{1, 2, 11, 12, 21, 22, 31, 32\}$, $T + 2$, $T + 4$, $T + 6$, $T + 8$.⁵⁷ From this it follows that \mathcal{C}_0 , of size $\#\mathcal{C}_0 = 6801$, can be extended by $10 + 4 \times 10 + 4 \times 8 + 4 \times 8 = 114$ planes in \mathcal{E} to a subspace code of size 6915.

Proceeding further as in the case $q = 2$, we find that the 4×4 arrays corresponding to $[L_1]$ and $[L_3]$ do not contain row-and-column transversals with all four 8-tuples distinct. Thus the argument used in the case $q = 2$ to extend the intermediate subspace code further by planes in \mathcal{N}'' breaks down and the situation becomes considerably more involved. We have conducted a non-exhaustive computer search for maximal extensions of \mathcal{C}_0 (a more general approach than only trying to further extend one particular extension of size 6915). As already mentioned, the largest extension found in this way has size $\#\overline{\mathcal{C}}_0 = 6977$.

7. CONCLUSION

We have developed the expurgation-augmentation approach to the construction of good subspace codes, originally presented in [21] and

⁵⁶This follows from the fact that the differences $0, \pm 2 \pmod{8}$ do not occur within the connection set $\{\pm 1, \pm 28, \pm 37, \pm 27, \pm 36, \pm 9\}$ of the circulant graph.

⁵⁷Similarly due to the fact that $0, \pm 1 \pmod{10}$ do not occur within the connection set $\{\pm 2, \pm 18, \pm 25, \pm 16, \pm 23, \pm 7\}$

later extended in [27], in greater depth, providing an explicit formula (in terms of the σ -invariant) for the number of new planes meeting the special solid S in a point that can be added to the expurgated lifted Gabidulin code without introducing a multiple cover of some line, and a much refined analysis of the final extension step by planes meeting S in a line.

The existence problem for q -analogues of the Fano plane, which provided a great deal of motivation for the present work, remains grossly open, but this will not discourage us, nor should it discourage anybody else in the audience, from further attempts to resolve it—at least in the case $q = 2$, for which by Moore’s Law a computer attack will become feasible in the not too distant future.

Should a q -analogue indeed exist, it may be possible to construct it using a variant of our approach, starting with either a non-Gabidulin MRD code or a smaller set of 3×4 matrices at pairwise rank distance ≥ 2 that cannot be embedded into an MRD code.⁵⁸

The present work may also be continued by investigating, for general q , the sizes of optimal decompositions of Singer line orbits of $\text{PG}(3, \mathbb{F}_q)$ into $q + 1$ partial spreads and how these should be wired to the points of the corresponding ovoid sections in W in order to maximize further extendability by planes in \mathcal{N}'' ; cf. the end of Section 6. This should narrow down the gap between the lower and upper bound for the size of a maximal extension $\overline{\mathcal{C}_0}$ given at the beginning of Section 6; cf. also Theorem 4 (iii).

Finally we believe that large portions of the machinery developed can be generalized to subspace codes of packet lengths $v > 7$. While for larger v there is no analogue of the trace-zero subspace W and hence no canonical choice for the ambient space and its corresponding σ -invariant, it should still be possible to derive by our method some explicit results on the number of planes in \mathcal{N}' that can be added to the expurgated subspace code, and to carry over the extension analysis in Section 6 to some extent.

REFERENCES

- [1] A. Beutelspacher. On parallelisms in finite projective spaces. *Geometriae Dedicata*, 3(1):35–40, 1974.
- [2] A. Beutelspacher. Partial spreads in finite projective spaces and partial designs. *Mathematische Zeitschrift*, 145:211–230, 1975. Corrigendum, *ibid.* 147:303, 1976.
- [3] A. Beutelspacher and U. Rosenbaum. *Projektive Geometrie*. Number 41 in Vieweg Studium. Vieweg, 1992.

⁵⁸When finishing up our work on plane subspace codes in $\text{PG}(5, \mathbb{F}_q)$, we have discovered that one of the five isomorphism types of optimal binary subspace codes of size 77 can be constructed from a set of 48 binary 3×3 matrices that is not extendable to an MRD code.

- [4] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, and A. Wassermann. Existence of q -analogs of Steiner systems. Preprint arXiv:1304.1462 [math.CO], Apr. 2013.
- [5] M. Braun and J. Reichelt. q -analogs of packing designs. *Journal of Combinatorial Designs*, 22(7):306–321, July 2014. Preprint arXiv:1212.4614 [math.CO].
- [6] P. J. Cameron. Generalisation of Fisher’s inequality to fields with more than one element. In *Combinatorics (Proc. British Combinatorial Conf., Univ. Coll. Wales, Aberystwyth, 1973)*, pages 9–13. London Math. Soc. Lecture Note Ser., No. 13. Cambridge Univ. Press, London, 1974.
- [7] P. J. Cameron. Note on large sets of infinite Steiner systems. *Journal of Combinatorial Designs*, 3(4):307–311, 1995.
- [8] P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25:226–241, 1978.
- [9] P. Dembowski. *Finite Geometries*. Springer-Verlag, 1968. Classics in Mathematics Series, 1997.
- [10] R. H. F. Denniston. Packings of $PG(3, q)$. In A. Barlotti, editor, *Finite Geometric Structures and their Applications*, number 60 in CIME Summer Schools, pages 195–199. Springer-Verlag, 2011. Reprint of the 1st ed. C.I.M.E., Ed. Cremonese, Roma, 1973.
- [11] G. L. Ebert. Partitioning projective geometries into caps. *Canadian Journal of Mathematics*, 37(6):1163–1175, 1985.
- [12] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence. The maximum size of a partial 3-spread in a finite vector space over $GF(2)$. *Designs, Codes and Cryptography*, 54(2):101–107, 2010.
- [13] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Transactions on Information Theory*, 55(7):2909–2919, July 2009.
- [14] A. Fazeli, S. Lovett, and A. Vardy. Nontrivial t -designs over finite fields exist for all t . Preprint arXiv:1306.2088 [math.CO], June 2013.
- [15] T. Feulner. The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes. *Advances in Mathematics of Communications*, 3(4):363–383, Nov. 2009.
- [16] T. Feulner. Canonical forms and automorphisms in the projective space. Preprint arXiv:1305.1193 [cs.IT], May 2013.
- [17] T. Feulner. *Eine kanonische Form zur Darstellung äquivalenter Codes – Computergestützte Berechnung und ihre Anwendung in der Codierungstheorie, Kryptographie und Geometrie*. Phd thesis, Universität Bayreuth, 2014.
- [18] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems of Information Transmission*, 21(1):1–12, 1985.
- [19] D. G. Glynn. On a set of lines of $PG(3, q)$ corresponding to a maximal cap contained in the Klein quadric of $PG(5, q)$. *Geometriae Dedicata*, 26(3):273–280, 1988.
- [20] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford University Press, 2nd edition, 1998.
- [21] T. Honold, M. Kiermaier, and S. Kurz. Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4. To appear in the proceedings volume of the 11th International Conference on Finite Fields and their Applications (Magdeburg, July 22–26, 2013), AMS Contemporary Mathematics Series, Vol. 632, 2015. Preprint arXiv:1311.0464 [math.CO], Nov. 2013.
- [22] P. Keevash. The existence of designs. Preprint arXiv:1401.3665 [math.CO], Jan. 2014.

- [23] M. Kiermaier and R. Laue. Derived and residual subspace designs. *Advances in Mathematics of Communications*, 9(1):105–115, Feb. 2015.
- [24] M. Kiermaier and M. O. Pavčević. Intersection numbers for subspace designs. *Journal of Combinatorial Designs*, published online, July 2014.
- [25] R. Koetter and F. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, Aug. 2008.
- [26] A. Kohnert and S. Kurz. Construction of large constant dimension codes with a prescribed minimum distance. In J. Calmet, W. Geiselmann, and J. Müller-Quade, editors, *Mathematical Methods in Computer Science. Essays in Memory of Thomas Beth*, number 5393 in Lecture Notes in Computer Science, pages 31–42. Springer-Verlag, 2008.
- [27] H. Liu and T. Honold. Poster: A new approach to the main problem of subspace coding. In *9th International Conference on Communications and Networking in China (ChinaCom 2014, Maoming, China, Aug. 14–16)*, pages 676–677, 2014. Full paper available as arXiv:1408.1181 [math.CO].
- [28] R. M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, Mar. 1991. Comments by Emst M. Gabidulin and Author’s Reply, *ibid.* 38(3):1183, 1992.
- [29] D. Silva, F. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, Sept. 2008.
- [30] L. Teirlinck. Non-trivial t -designs without repeated blocks exist for all t . *Discrete Mathematics*, 65(3):301–311, 1987.
- [31] S. Thomas. Designs over finite fields. *Geometriae Dedicata*, 24:237–242, 1987.
- [32] A.-L. Trautmann and J. Rosenthal. New improvements on the Echelon-Ferrers construction. In A. Edelmayer, editor, *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010)*, pages 405–408, Budapest, Hungary, 5–9 July 2010. Reprint arXiv:1110.2417 [cs.IT].

DEPARTMENT OF INFORMATION SCIENCE AND ELECTRONICS ENGINEERING,
 ZHEJIANG UNIVERSITY, 38 ZHEDA ROAD, 310027 HANGZHOU, CHINA
E-mail address: honold@zju.edu.cn

MATHEMATISCHES INSTITUT, UNIVERSITÄT BAYREUTH, D-95440 BAYREUTH,
 GERMANY
E-mail address: michael.kiermaier@uni-bayreuth.de